

PRIVACY LAW



presents

Annual Privacy Summit

MCLE: 1.0 Hours

Day 2- Track 1- Panel 4- Focus on Data Brokers: California's DELETE Act and Other Developments

Friday, February 9th, 2024
2:30 p.m. – 3:30 p.m.

Speakers:

Tom Kemp

Ben Isaacson

Meghan Land

Lothar Determann

Conference Reference Materials

Points of view or opinions expressed in these pages are those of the speaker(s) and/or author(s). They have not been adopted or endorsed by the California Lawyers Association and do not constitute the official position or policy of the California Lawyers Association. Nothing contained herein is intended to address any specific legal inquiry, nor is it a substitute for independent legal research to original sources or obtaining separate legal advice regarding specific legal situations.

© 2020 California Lawyers Association
All Rights Reserved

The California Lawyers Association is an approved State Bar of California MCLE provider.

The Employer Report

NAVIGATING US AND GLOBAL EMPLOYMENT LAW

Employers Must Prepare Now For New California Employee Privacy Rights

**Baker
McKenzie.**

By Guest Contributor on January 3, 2022

Many thanks to [Lothar Determann](#) and [Jonathan Tam](#) for this post.

Some of your job applicants and employees in California may be alarmed if you tell them you sell their personal information. But you will have to say you sell their personal information if you disclose their personal information to third parties after January 1, 2022 without including certain data processing clauses in your contracts, as required by the California Consumer Privacy Act (CCPA). So we recommend reviewing these contracts to ensure they include the prescribed clauses if you wish to avoid being a “seller” of personal information.

You should also get ready to field data access, deletion, correction, portability and other requests from your employees and other personnel in California starting January 1, 2023. This will require implementing new protocols and training up your human resources and compliance teams. We also recommend tightening up your data retention and deletion protocols to limit the amount of information you have to review when handling data subject requests.

Do you use employee monitoring software or algorithms to help you evaluate job applicants? You should ensure that your use of these and similar tools address upcoming requirements regarding automated decision-making, risk assessments and the use of sensitive personal information. Note that the CCPA also currently requires employers to issue privacy notices to their California employees pursuant to a California Privacy Rights Act (CPRA) amendment that took effect on December 16, 2020.

There is an HR exception under the CCPA but it is not comprehensive and expires January 1, 2023. When the CCPA originally passed in 2018, it included a limited, temporary carve-out for personal information of job applicants, employees, independent contractors and other personnel, who only needed to receive a brief “notice at collection.” The CPRA extended the limited carve-out until January 1, 2023 and immediately expanded the list of disclosures that employers have to provide to employees and candidates at or before the time of collecting their personal information. [1] Such “notices at collection” must include details about the types of personal information collected, the purposes for which the information is collected, and how long the personal information is retained or the criteria for determining the same. The California Attorney General’s CCPA Regulations also require notices at collection to indicate whether the business sells California residents’ personal information and a notice of the their right to opt-out of sales if so, and a link to the business’s privacy policy.[2] You should begin to address these requirements immediately if you have not done so already.

Starting in 2023, you will be fully subject to CCPA requirements with respect to your California job applicants and personnel.

Here are some key recommendations.[3]

1. **Review your agreements with third-party recipients of personal information.** The CCPA prescribes certain types of clauses that will have to appear in agreements between parties exchanging personal information, and you will have to include certain data processing clauses if you do not want to be considered to be “selling” or “sharing” (which the CCPA defines to mean disclosing for the purposes of cross-context behavioral advertising) personal information. We recommend broaching these requirements with your business partners as soon as possible if you have not already done so, given the time needed to negotiate contracts and the fact that you have to disclose your practices in the prior 12 months, i.e., after January 1, 2022.
2. **Implement data subject request protocols and tighten up record retention and data deletion protocols.** California job applicants and personnel will gain data access, portability, correction, deletion and other rights in 2023. You should implement protocols and training to ensure that your HR, compliance and similar teams can deal with their requests in a consistent, timely and compliant manner. Any email, spreadsheet, contract or other document that refers to a California-based employee constitutes their “personal information” which you may have to produce in response to an access request, free of charge. To keep track of where information is stored while reducing the amount of data potentially subject to data access requests, you should work on tightening your data retention and deletion protocols. This will also help you comply with CCPA’s new data minimization requirements.[4]

3. **Consider whether and the extent to which you process “sensitive personal information”, such as if you use employee monitoring software, and address related CCPA requirements.** California residents will have the right to request that businesses stop using their “sensitive personal information” for purposes outside of various narrow exceptions.[5] CCPA defines “sensitive personal information” to include, among other things, government identifiers, precise geolocation data, information on racial or ethnic origin, religious or philosophical beliefs, and the contents of a California resident’s mail, email and text messages addressed to someone other than the business. If you process sensitive personal information outside of the excepted purposes, you have to post a link titled “Limit the Use of my Sensitive Personal Information” online. CCPA may also require you to engage in privacy risk assessments and allow California residents to opt-out of automated decision-making activities in certain situations. The newly established California Privacy Protection Agency will clarify these requirements when it promulgates its CCPA regulations next year, and we recommend that you stay abreast of such developments to ensure that your HR data processing activities comply.
4. **Update privacy policy and privacy notices.** Your privacy policy will have to reflect your processing of HR data. You should consider preparing a privacy policy that is specific to CCPA and separate from any privacy policy you might use to address privacy laws in other jurisdictions, since California laws establish unique requirements and use unique terms that may be difficult to reconcile with those of other jurisdictions. At the same time, you have to be mindful of setting or negating privacy expectations. If you issue privacy notices to job applicants and personnel that merely address CCPA disclosure requirements, the recipients of such notices may develop limited privacy expectations that could later hinder you in conducting investigations or deploying monitoring technologies intended to protect data security, co-workers, trade secrets and compliance objectives.[6]

Outlook and Practical Guidance

The California Privacy Protection Agency has started the process of drafting regulations by July 1, 2022 specifying how certain requirements under the revised CCPA apply. Most large and medium-sized companies that do business in California will be impacted. Compliance with the European Union General Data Protection Regulation (GDPR) or other jurisdictions’ privacy or data protection laws is not sufficient to meet requirements under the revised CCPA, which are prescriptive and require companies to use counterintuitive terminology on website links and in privacy notices.

The California Attorney General’s Office currently enforces CCPA, and the California Privacy Protection Agency will have the power to bring administrative enforcement actions under CCPA starting July 1, 2023. The authorities can investigate violations, hold hearings, issue cease-and-

desist orders, and impose administrative fines of up to \$7,500 for each intentional violation. Currently, CCPA requires the California Attorney General's Office to give a business a 30-day cure period before bringing enforcement actions. Starting July 1, 2023, the California Attorney General's Office and California Privacy Protection Agency will be able to bring enforcement actions without delay.

For more details see, [Lothar Determann, California Privacy Law](#) and [Determann's Field Guide to Data Privacy Law](#).

[1] See Section 31 of the CPRA ("Subdivisions (m) [...] of Section 1798.145 [of the California Civil Code ...] shall become operative on the effective date of the [California Privacy Rights Act]"). Subdivision (m) of Section 1798.145 of the California Civil Code sets forth the HR exception but also states that the exception "shall not apply to subdivision (a) of Section 1798.100". One of the original drafters of the CPRA clarified that this reference is intended to refer to subdivision (a) of Section 1798.100, as amended by the CPRA. Subdivision (a) of Section 1798.100 of the California Civil Code, as amended by the CPRA, sets forth a requirement to provide California residents with a privacy notice at or before collection of their personal information. See also California Privacy Experts Break Down the CPRA, the Recorder, December 28, 2020, available at: <https://www.law.com/therecorder/2020/12/28/california-privacy-experts-break-down-the-cpra/?slreturn=20211129180107>.

[2] 11 CCR § 999.305.

[3] For an in-depth breakdown of new CCPA requirements, please see "United States: The California Privacy Rights Act of 2020 – A broad and complex data processing regulation that applies to businesses worldwide", Lothar Determann and Jonathan Tam, <https://insightplus.bakermckenzie.com/bm/data-technology/united-states-the-california-privacy-rights-act-of-2020-a-broad-and-complex-data-processing-regulation-that-applies-to-businesses-worldwide>.

[4] Cal. Civ. Code § 1798.100(c). For general guidance on developing personal information retention protocols, please see *How to Develop a Privacy -Enriched Data Retention Policy*, Theo Ling and Jonathan Tam, Canadian Privacy Law Review, Volume 17, Number 8, July 2020, available [here](#) (last accessed October 31, 2021).

[5] Cal. Civ. Code § 1798.121.

[6] Lothar Determann and Robert Sprague. Berkeley Technology Law Journal Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States.



The Employer Report



Copyright © 2022, Baker & McKenzie LLP. All Rights Reserved.

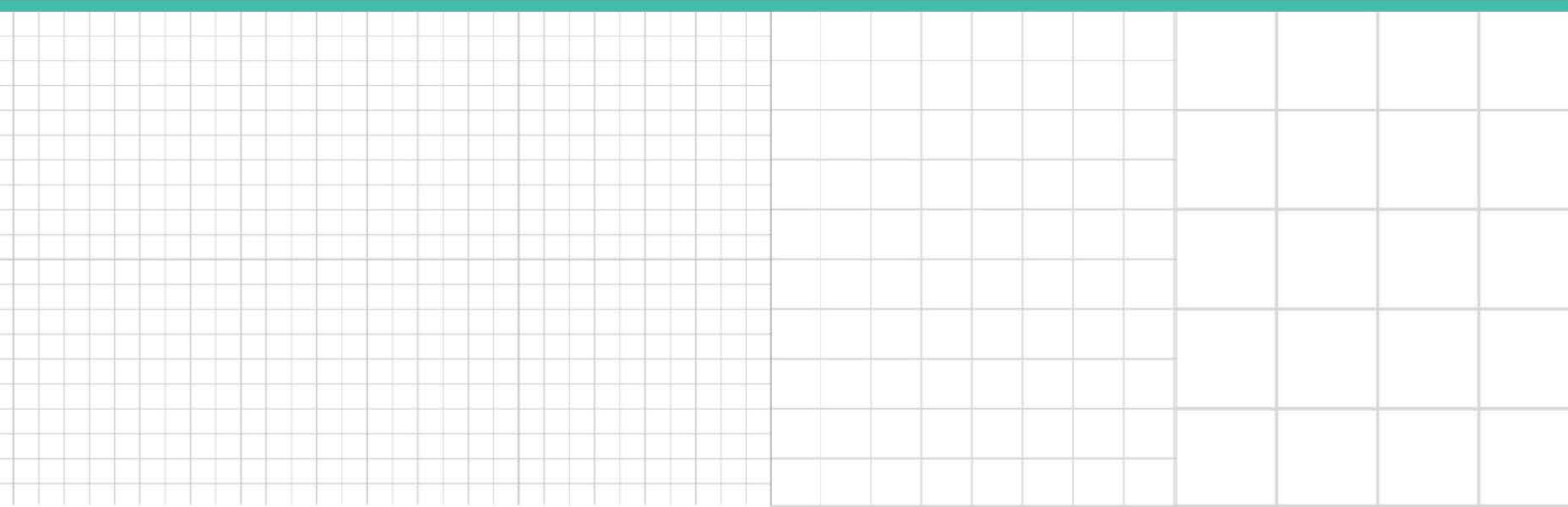


Professional Perspective

CCPA Litigation Trends

*Lothar Determann and Teresa Michaud,
Baker McKenzie*

Reproduced with permission. Published September 2020. Copyright © 2020 The Bureau of National Affairs, Inc. 800.372.1033. For further use, please visit: <http://bna.com/copyright-permission-request/>



CCPA Litigation Trends

Contributed by [Lothar Determann](#) and [Teresa Michaud](#), Baker McKenzie

On July 1, 2020 California's attorney general started enforcing the California Consumer Privacy Act by sending letters to companies with requests to cure alleged violations, as contemplated by the [CCPA](#). The legislation took effect on Jan. 1, 2020, as part of the California Civil Code, and called on the attorney general to enforce the law within six months of enacting regulations or July 1, 2020 the latest. The CCPA regulations became final only on Aug. 14, 2020, and the attorney general announced that they would apply with immediate effect on the same day.

Despite a seemingly clear division between the domains of government and private enforcement, plaintiffs' attorneys have been busy exploring ways that the CCPA can supply a basis for private civil litigation outside the data breach context. Whether private plaintiffs will be successful in this attempted expansion of the CCPA remains to be determined, but current trends in CCPA litigation can provide insight on what might be in store. This article explores those trends.

Within the CCPA, subsection (a) of [Cal. Civ. Code § 1798.150](#) creates a narrowly framed right to private action in case of certain security breaches and clarifies in subsection (c) that aside from this one cause of action, "nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." By design, the CCPA vests enforcement authority in the attorney general.

We begin by examining a few selected lawsuits asserted under the data breach private right of action ([Cal. Civ. Code § 1798.150](#)), as the statute expressly contemplates. We then summarize some of the CCPA-related legal theories in non-data breach lawsuits, grouped generally into three main categories: unfair competition law claims based on underlying violations of the CCPA, negligence per se claims incorporating various apparent CCPA standards of care, and actions asserted directly under the CCPA.

Certainly, courts will have to determine whether these non-data breach legal claims can survive demurrer or motions to dismiss. None of the cases discussed herein have progressed yet to the extent that defendants have filed meaningful responsive pleadings, such as an answer to the allegations or a motion to dismiss pursuant to Rule 12(b)(6), much less to the point where a court decision has been issued.

Data Breach Claims Under Private Right of Action

[Cal. Civ. Code § 1798.150\(a\)](#) of the CCPA allows any California resident to institute a civil action for monetary and injunctive relief if their personal information (a narrow category defined by the act) is subject to the "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," circumstances commonly referred to as a "data breach." The following lawsuits have asserted data breach claims under section 1798.150.

In re: Hanna Andersson, et al. Data Breach Litigation, N.D. Cal. (Master File No. 3:20-cv-00812)

The plaintiffs in this consolidation [action](#) seek to represent a nationwide class, as well as a California sub-class of customers whose names, addresses and credit card information were allegedly exposed, "scraped," and offered for sale on the "dark web" following an alleged data breach suffered by Hanna Andersson in 2019, before the CCPA took effect. The plaintiffs' section 1798.150 claim alleges that the defendants failed to prevent the plaintiffs' and California sub-class members' unencrypted and non-redacted personally identifiable information (PII) from "unauthorized access and exfiltration, theft, or disclosure." The plaintiffs sued not only Hanna Andersson, with whom they had direct business dealings, but also a service provider, with whom the plaintiffs had no contractual or other relationships, despite the fact that the CCPA imposes obligations and liability only on businesses, not their service providers.

The plaintiffs alleged injuries including: "lost or diminished value of PII," "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII," "lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to lost time," "deprivation of rights they possess under ... the California Consumer Privacy Act ([Cal. Civ. Code § 1798.100](#), et seq.)," and "the continued and certainly an increased risk to their PII."

On Aug. 17, 2020, before the defendants had even filed a Rule 12 motion or otherwise responded to the plaintiffs' substantive allegations, the court stayed the case for 30 days following the parties' notice of settlement.

Fuentes v. Sunshine Behavioral Health Group, LLC, C.D. Cal. (Case No. 8:20-cv-00487)

The plaintiff here [alleges](#) that Sunshine, a drug and alcohol rehabilitation facility, allegedly violated the CCPA in connection with an alleged data breach that occurred in September 2019, before the CCPA took effect, and allegedly exposed the sensitive personal and medical information of approximately 3,500 patients. The named plaintiff is not a California resident, but a resident of Pennsylvania who was in California when the alleged breach occurred, and seeks relief under section 1798.150 in addition to California's Confidentiality of Medical Information Act ([CMIA](#)).

The plaintiff further seeks class-wide injunctive relief "in the form of an order enjoining Defendant from continuing to violate the CCPA." The complaint continues that should Sunshine not respond to the plaintiff's CCPA violation notice letter and rectify the alleged violation, the plaintiff "will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations." Notably, [Cal. Civ. Code § 1798.145\(c\)\(1\)](#) states that CCPA shall not apply to personal information governed by CMIA or HIPAA.

Brodsky v. Ambry Genetics, Corp., C.D. Cal. (Case No. 8:20-cv-00811)

The plaintiff [asserts](#) a putative class action based on the alleged inadvertent disclosure of HIPAA-protected consumer information, including patients' names, dates of birth, health insurance information, medical information, and for some patients, Social Security numbers, and other sensitive personal information and Protected Health Information (PHI). While the complaint references that the plaintiff, "on behalf of all others similarly situated, alleges claims for ... violation of the California Consumer Privacy Act ([Cal. Civ. Code § 1798.100](#), et seq. (§ 1798.150(a)))," it stops short of actually seeking monetary or injunctive relief under the CCPA's private right of action.

Nevertheless, the court in June 2020 ordered that the *Brodsky* complaint be consolidated with three other related actions against the same defendant, which may well lead to an amended pleading that includes a standalone section 1798.150 claim. Again however, [Cal. Civ. Code § 1798.145\(c\)\(1\)](#) states that CCPA shall not apply to personal information governed by CMIA or HIPAA.

Cercas, et al. v. Ambry Genetics Corp., C.D. Cal. (Case No. 8:20-cv-00791)

This consolidated [action](#) consists of separate individual complaints alleging that the defendant, a genetic testing facility, failed to implement and maintain reasonable data security measures. At least one complaint asserts a claim against the defendant for violating the CCPA by noting that the unauthorized access of unencrypted and non-redacted personal and medical information was a result of the defendant's duty to implement and maintain such measures. The parties have proposed a deadline of Nov. 20, 2020 for the defendant to file a responsive pleading.

Karter v. Epiq Systems, Inc., Orange County Superior Court (Case No. 30-2020-01145269)

The putative class action [complaint](#) in this case asserts a sole claim against a legal services technology provider for a violation of the CCPA. The plaintiff seeks relief under section 1798.150 for the defendant's alleged use of outdated data security measures, leading to various malware and ransomware attacks and the exfiltration of consumers' unencrypted and non-redacted personal information.

Gupta, et al. v. Aeries Software, Inc., C.D. Cal. (Case No 8:20-cv-00995)

The plaintiffs, an individual and his minor children, [assert](#) claims against a software company that manages student-data for failing to implement adequate data security measures, failing to detect a data breach, and failing to maintain security systems consistent with industry standards. The complaint further alleges that the defendant owed a heightened duty to the plaintiffs as minors, and that the data security shortcomings resulted in a data breach of the minors' personal information. The plaintiffs rely on alleged violations of the CCPA to an unfair competition law claim in addition to their section 1798.150 data breach cause of action.

California Unfair Competition Law Claims Asserting Violations

California's unfair competition law provides a private right of action arising from, among other things, any "unlawful conduct." The plaintiffs have brought unfair competition law claims on the theory that defendants have acted unlawfully by

violating various aspects of the CCPA other than section 1798.150's data breach provisions. As indicated above, enforcement of these additional aspects of the CCPA is reserved for the California attorney general, not private litigants.

Indeed, section 1798.150(c) explains that the CCPA's private cause of action "shall not be based on violations of any other section" of the law, "nor shall a CCPA violation "be interpreted to serve as the basis for a private right of action under any other law." The statute therefore would seem clearly to bar a "private right of action under" the unfair competition law whose basis is an alleged violation of the CCPA. Yet this has not prevented plaintiffs from testing the boundaries of this straightforward statutory limitation.

Burke, et al. v. Clearview AI, Inc., et al., S.D.N.Y., originally filed in S.D. Cal., case no. 3:20-cv-00370 (Case No. 1:20-cv-03104)

The plaintiffs [allege](#) that Clearview and its two founders used facial recognition technology to scrape social media websites for images of consumers' faces without their notice or consent, which they claim constitutes improper collection and sale of information protected by the CCPA. The plaintiffs' unfair competition law claim on behalf of various subclasses arises from the defendant's allegedly "unlawful" violation of the CCPA in collecting the class members' personal information without prior notice or consent. While the parties have battled over the proper venue for the case, the legal sufficiency of plaintiffs' unfair competition law claim has not yet been challenged.

Hernandez v. PIH Health Inc., Los Angeles County Superior Court (Case No. 20STCV09237)

The plaintiff [asserts](#) a number of claims arising out of a targeted phishing campaign against PIH, a regional healthcare network. The complaint alleges that the cyberattack against PIH affected the plaintiff and approximately 200,000 other individuals, and resulted the unauthorized disclosure of the plaintiff's medical information. But instead of asserting a section 1798.150 data breach claim, the Complaint alleges that PIH's potential violation of the CCPA gives rise to liability under California's unfair competition law.

Alizadeh, et al. v. Enloe Medical Center, Butte County Superior Court (Case No. 20cv00799)

The plaintiffs in this [case](#) assert a host of claims against an operator of medical facilities in response to a ransomware attack against the defendant. The allegations state that the ransomware attack blocked access to highly sensitive patient medical records, and that putative class members suffered losses in the form of disrupted medical services and other expenses. The complaint alleges that failures to protect against the attack resulted in violations of multiple laws, including the CCPA, and that these violations in turn support an unfair competition law claim.

Bombora, Inc. v. ZoomInfo Technologies LLC, Santa Clara County Superior Court (Case No. 20CV365858)

In this [case](#) between two data brokers, the plaintiff alleges that the defendant, a former business partner, gains competitive advantages by violating the CCPA. Both companies sell so-called "intent" data, which purportedly attempts to predict consumers' future product purchases. The complaint alleges that the defendant does not include an opt-out notification regarding the data it collects within a "free" user application, and that this policy violates the CCPA and therefore supports a claim under unfair competition law. The defendant has filed a motion to dismiss arguing that a forum selection agreement between the parties mandates suit in federal or state court in New York, New York.

Negligence Per Se Claims Alleging Violations of Statutory Duties of Care

As described above, section 1798.150 of the CCPA allows private litigants whose data has been subjected to unauthorized access to seek damages arising from a business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." This is, in effect, a statutory duty of care—albeit bereft of any clear guidance as to what constitutes "reasonable security procedures and practices"—which could theoretically provide the basis for a common law "negligence per se" theory of liability.

Indeed, in the *Hanna Andersson* litigation discussed above, one of the plaintiffs originally included a claim sounding in negligence per se, alleging that the defendants had breached section 1798.150's duty of care in the protection of consumers' personal information. The plaintiff subsequently voluntarily dismissed that claim, presumably because the CCPA provides for statutory damages; in common law negligence claims involving data breach events, proving causation and damages can be very difficult.

The cases described below have asserted a similar theory of negligence liability. We believe, however, that such claims should be subject to dismissal for the same reasons discussed above in connection with unfair competition law: the CCPA by its own terms may not “be interpreted to serve as the basis for a private right of action under any other law,” including the common law of negligence.

Henrichsen, et al. v. Tandem Diabetes Care, Inc., S.D. Cal. (Case No. 3:20-cv-00732)

This putative class [action](#) is brought by an Illinois plaintiff, her minor son, and a California plaintiff against a medical device manufacturer. The plaintiffs allege that a phishing attack caused a data breach, and they accuse the defendant manufacturer of failing to implement and maintain reasonable security procedures and practices to prevent such a breach. The plaintiffs assert a section 1798.150 data breach cause of action, as well as claims for negligence and unfair competition law violations predicated on alleged CCPA violations. On May 22, 2020, the plaintiffs voluntarily dismissed their lawsuit, but without prejudice to refile it in the future.

Atkinson, et al. v. Minted, Inc., N.D. Cal. (Case No. 3:20-cv-03869)

The plaintiffs here [seek](#) to represent a consumer class against the defendant, an online marketplace for “crowd sourced” home goods, for an alleged data breach and disclosure of their PII. In addition to asserting a section 1798.150 data breach claim, the plaintiffs rely upon the duties imposed under the CCPA to accuse the defendant of negligence per se. The plaintiffs also assert an unfair competition law claim based on alleged CCPA violations.

Juan Flores-Mendez, et al. v. Zoosk Inc., et al., N.D. Cal. (Case No. 3:20-cv-04929)

Two plaintiffs [allege](#) that the defendant, the creator and manager of an online dating app, failed to implement and maintain reasonable security measures, which resulted in the hacking and theft of users’ information. The complaint alleges that putative class members must constantly monitor personal records as a result of the data breach and that they are now at higher risk of phishing and pharming attacks. The plaintiffs include a claim under the CCPA itself for the company's alleged failures, but additionally use the statute to support negligence and unfair competition law claims.

Non-Data Breach Claims

In this last category of cases, the plaintiffs seek to base claims directly on allegations of defendant's failure to comply with the CCPA's consumer notification and consent provisions. The plaintiffs do not invoke unfair competition law or other causes of action to support their claims with indirect references to CCPA violations, as in the previously discussed group of cases, but plaintiffs refer directly to CCPA sections, despite the fact that [Cal. Civ. Code § 1798.150\(c\)](#) expressly and specifically precludes such claim.

In re Ring LLC Privacy Litigation, C.D. Cal. (Case No. 2:19-cv-10899)

This consolidated [action](#) includes class claims by a Washington consumer against a video doorbell and security camera manufacturer. At least one of the related cases (Case No. 20-cv-01538) includes a standalone cause of action for “violation” of the law for allegedly collecting and using personal information without providing consumer notice and an opportunity to opt out.

Sweeney v. Life on Air, Inc., et al., S.D. Cal. (Case No. 3:20-cv-00742)

The California plaintiff here [asserts](#) claims on behalf of a putative class against two companies behind a social networking application that allows for multiple users to video chat simultaneously. The complaint alleges that the companies violated the CCPA by disclosing users’ PII to unauthorized third parties, including advertisers, without providing the required notice to and consumers and giving them a right to opt out. Interestingly, despite its many CCPA-related allegations, the complaint does not rely on that statute in asserting liability under California's unfair competition law. The defendants have responded by filing a motion to compel arbitration or alternatively transfer the case.

L.P., et al. v. Shutterfly Inc., N.D. Cal. (Case No. 3:20-cv-04960)

A group of minors brought [suit](#) against the defendant, an online image sharing platform, for alleged violations regarding the company's facial recognition software. The plaintiffs allege that the company used the software on users and non-users to “tag” them in photos without consent, concealed its use of the software, failed to disclose the collection of biometric data, and then sold personal information of minors to third parties. The complaint asserts a direct violation of CCPA on the

theory that the “sale of personal information of minors equates to that of a data breach,” thereby stretching the statutory definition of data breach past its likely breaking point.

Insights from Pending Cases

In the cases filed to date, the plaintiffs’ attorneys have not advanced any compelling arguments why the clear limitations on private actions in the CCPA should not apply and preclude the claims. The claims based on unfair competition law and negligence per se clearly fall within the CCPA prohibition that “Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.” Courts have not yet allowed any such cases to proceed in litigation past the motion to dismiss stage.

Ed Totino, Alex Davis, Sara Pitt, Gary Hunt, and Tom Tysowsky contributed to this article.

30 Aug 2023



Data & Technology

United States: Senate Bill 362 to amend California Data Broker Law

United States: Senate Bill 362 to amend California Data Broker Law

30 Aug 2023 2 minute read

[CPPA](#) | [Senate Bill 362](#) |

In brief

If you are a data broker or a business that relies on data brokers for targeted advertising, you should be aware that the California [Data Broker Law](#) may be significantly changed under a proposed bill. Under [Senate Bill 362](#), the California Privacy Protection Agency (CPPA) would be required to set up, by January 1, 2026, an accessible deletion mechanism where consumers could request deletion via the CPPA that all data brokers then have to honor. Data brokers would have to check the CPPA mechanism to process all deletion requests every 31 days, as well as delete personal information about every California resident who ever made a request through the mechanism every 31 days.

Should the bill pass, it could profoundly impact how data brokers handle personal information and subsequently impact the businesses that partner with data brokers for targeted advertising.

Contents

Where we are right now

Currently, data brokers seem to remain a foot away from the fire: California Civil Code § 1798.99.80, et seq., just require data brokers to register with the Attorney General and pay an annual registration fee. In registering with the Attorney General, data brokers are required to provide its name, primary physical, email, and internet website addresses.

What Senate Bill 362 is proposing

Senate Bill 362 would add additional obligations by introducing a single “accessible deletion mechanism,” provided online by the CPPA. Consumers would be able to use such mechanism to request that every data broker that maintains any personal information about the consumer delete such personal information held by the data brokers or associated service providers or contractors. The data brokers would be required to process deletion requests that are made through the CPPA mechanism within 31 days of receiving them,

and beginning July 1, 2026, continuously delete the personal information of the requesting consumer and not sell or share new personal information of the consumer. Data brokers would also be required to direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the requesting consumer. This means that California consumers would be able to request deletion of any and all personal information maintained by different data brokers with just a single deletion request.

The bill would also require data brokers to provide additional information to the CPPA when registering as data brokers, including to specify whether they collect the personal information of minors, consumers' precise geolocation, and consumers' reproductive health care data. Data brokers would also be required to maintain a website free of dark patterns that details how consumers may exercise their privacy rights. Beginning January 1, 2028, and every three years thereafter, data brokers would be required to submit an audit report to the CPPA upon the CPPA's written request.

Senate Bill 362 would also replace the Attorney General with the CPPA as the authority tasked with enforcing the Data Broker Law. The CPPA is the same agency that implements and, together with the California Attorney General, enforces the CCPA.

What this means

Should California consumers extensively use this deletion mechanism, this could reduce the size of a data broker's database. Partnering businesses that rely heavily on data brokers for their marketing initiatives might feel a ripple effect with less effective targeted advertising.

Looking forward

Should Senate Bill 362 become law, data monetization in California faces another blow as data brokers would be subject to additional obligations under the streamlined deletion mechanism for California consumers. The extent of consumer engagement with the mechanism will play a determining role in the impact of the bill.

Contact Information

Lothar Determann

Partner

Palo Alto

[Read my Bio](#)

lothar.determann@bakermckenzie.com

Jonathan Tam

Partner

San Francisco

[Read my Bio](#)

jonathan.tam@bakermckenzie.com

Helena Engfeldt

Partner

San Francisco

[Read my Bio](#)

helena.engfeldt@bakermckenzie.com

Michelle Shin

Associate

San Francisco

[Read my Bio](#)

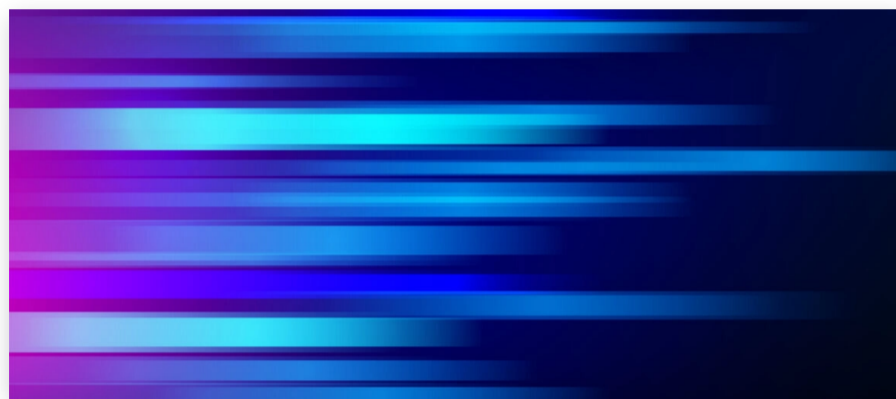
michelle.shin@bakermckenzie.com

Copyright © 2023 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.

CALIFORNIA PRIVACY LAW

California Consumer Privacy Act Regulations Closer to Finalization – 7 Takeaways

FEBRUARY 7, 2023 by JONATHAN TAM, LOTHAR DETERMANN AND HELENA ENGFELDT - 7 MINS READ



SHARE



Finalized regulations under the amended California Consumer Privacy Act (“CCPA”) are one step closer to becoming a reality. On February 3, 2023, the California Privacy Protection Agency (the “Agency”) voted to submit its **proposed regulations** to the Office of Administrative Law, which is one of the last steps before the regulations become law. The Office of Administrative Law will review the proposed regulations to ensure they are clear, necessary and based on valid legal authority. Further modifications may be necessary as the draft rules move toward the finish line. Nevertheless, we expect the current version of the proposed regulations to be a good proxy for the finalized version. This is because the amended CCPA grants the Agency broad authority to formulate its own regulations, and the Office of Administrative Law proposed few substantive edits to the California Attorney General’s proposed CCPA regulations in 2020. Below we outline 7 key takeaways from the Agency’s proposed regulations if they are adopted in their current form.

1. **A business must obtain a California resident’s consent to process their personal information for purposes outside of the CCPA’s “data minimization” criteria.** The CCPA and proposed regulations do not use the term “data minimization,” but we use the term to refer to Cal. Civ. Code § 1798.100(c), which requires a business’ personal information processing to be “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.” The Agency’s proposed regulations outline a series of factors that a business must consider when assessing whether the business’ processing will meet these criteria. Businesses should document their data minimization assessments in writing to support that the criteria are met. Where these criteria are not met, the regulations require a business to obtain the data

subject's consent before engaging in the processing. Consent must be specific, informed, unambiguous and given freely without the use of dark patterns (see #2 below). Acceptance of general or broad terms of use or similar document does not constitute consent.

2. **A business must avoid using dark patterns when seeking consent or offering data subject rights.** U.S. regulators are increasingly using the term "**dark patterns**" as a catch-all to cover a variety of misleading, deceptive or unfair practices, but the Agency provides some relatively structured guidance on how to avoid the use of dark patterns. In particular, the regulations require a business' methods for obtaining consent or submitting CCPA data subject requests to be easy to understand, symmetrical in choice, straightforward, non-manipulative, and easy to execute. The regulations provide some explanations and examples that help to clarify what these principles mean in practice.
3. **A business should carefully review the regulations when drafting privacy notices.** The Agency's CCPA regulations define five main classes of privacy notices that businesses must provide: (1) Notices at Collection; (2) Notice of Right to Limit; (3) Notice of Right to Opt-out of Sale/Sharing; (4) Notice of Financial Regulation; and (5) a Privacy Policy. The regulations enumerate the elements that the Agency expects to see in each of these classes of privacy notices. Not all of the elements enumerated in the regulations are found in the statutory text of the CCPA. For example, the regulations state that a Notice at Collection must include a link to the business' Privacy Policy. The regulations also prescribe how and where these notices must be provided to California residents. Because the privacy notices that a business must provide under the CCPA may vary substantially from those that the business provides to comply with other laws, businesses should consider whether to draft privacy notices addressed specifically to California residents for the purposes of complying with the CCPA, and should consider structuring the notices so that they present required information in the same order that the Agency's regulations list elements required to be included in notices.
4. **Service providers, contractors and third parties must also delete personal information in response to data subject requests.** The Agency's regulations make it clear that a business that gives effect to a California resident's request to delete personal information must also instruct its service providers and contractors to delete the personal information, and that these service providers must delete the personal information and instruct their own downstream service providers and contractors to delete the personal information. If the business sold or shared personal information to third parties, it must also instruct those third parties to delete the personal information unless doing so would be impossible or involves disproportionate effort. The regulations define "disproportionate effort" to mean, essentially, where the time and resources required to respond to the request would significantly outweigh the reasonably foreseeable impact to the data subject by not responding, and the definition specifically states that a business, service provider, contractor or third party that has failed to implement "adequate processes and procedures" to receive

and process data subject requests “cannot claim that responding” to a request would involve disproportionate effort.

5. **A business that sells or shares personal information must honor opt-out preference signals as a valid request to opt-out of selling or sharing.** For the business to be required to honor the **opt-out preference signal**, the signal must meet the following conditions: (1) It must be in a format commonly used and recognized by businesses, such as an HTTP header field or JavaScript object; and (2) The technology that sends the signal must make clear to users that sending the signal is meant to have the effect of opting them out of the sale and sharing of their personal information. The regulations include detailed rules about how to interpret an opt-out preference signal in different circumstances, such as if the business can only associate the signal with a browser or device but not a particular individual, or if the signal clashes with the individual’s participation in a business’ financial incentive program. The regulations also impose detailed technical requirements on businesses that wish to process opt-out preference signals in a “frictionless manner.” A business that processes opt-out preference signals in a frictionless manner can consolidate some of its CCPA disclosures and methods of receiving opt-out requests.
6. **A business should carefully review the regulations when negotiating data-related provisions with other parties.** The CCPA requires businesses to include certain elements in their contracts with service providers, contractors and third parties to whom they disclose personal information or de-identified information, sell personal information, or share personal information for cross-context behavioral advertising. The regulations include some examples of what these elements should entail. For example, the CCPA requires the business to reserve the contractual right to take reasonable and appropriate steps to stop and remediate the recipient’s unauthorized use of personal information. The proposed regulations indicate that a business may satisfy this requirement by obliging the recipient to produce documentation that verifies that it has honored a data subject request if the business instructs the recipient to comply with the request.
7. **The Agency has shed light on its enforcement procedures and powers.** For example, the Agency appears to commit to responding to every sworn complaint regarding an alleged violation of the CCPA. The Agency has also reserved broad powers to investigate, audit and commence enforcement proceedings against persons alleged to have violated the CCPA.

Many of the underlying CCPA requirements on which the Agency’s regulations expound have been in force since January 1, 2023, so companies have had to pursue compliance despite significant uncertainty around the applicable rules. Even if one round of finalized regulations now appears imminent, companies will have to continue to navigate an uncertain regulatory landscape since the Agency has signaled that it will release additional CCPA regulations in the future, including with respect to privacy and security risk assessments and automated decision-making technology.



Jonathan Tam

Jonathan Tam is a partner in the San Francisco office focused on global privacy, advertising, intellectual property, content moderation and consumer protection laws. He is a qualified attorney in Canada and the U.S. passionate about helping clients achieve their commercial objectives while managing legal risks. He is well versed in the legal considerations that apply to many of the world's cutting-edge technologies, including AI-driven solutions, wearables, connected cars, Web3, DAOs, NFTs, VR/AR, crypto, metaverses and the internet of everything.



Lothar Determann

Lothar has been helping companies in Silicon Valley and around the world take products, business models, intellectual property and contracts global for nearly 20 years. He advises on data privacy law compliance, information technology commercialization, interactive entertainment, media, copyrights, open source licensing, electronic commerce, technology transactions, sourcing and international distribution at Baker McKenzie in San Francisco & Palo Alto.



Helena Engfeldt

Helena practices international commercial law with a focus on assisting and advising technology companies with cross-border transactions, drafting and negotiating commercial agreements, and advising on global data privacy law compliance. Helena also advises software developers, e-commerce companies, and global mobile and web gaming developers on regulatory restrictions, intellectual property, contracting and data privacy.



Related Posts

User-enabled privacy controls under CCPA regulations

JANUARY 5, 2023

Virginia Consumer Data Protection Act takes effect in 2023

NOVEMBER 28, 2022

Employers preparing for CCPA compliance, what to do now

NOVEMBER 9, 2022



© Copyright 2023 – Connect On Tech

[Disclaimers](#) | [Privacy Statement](#) | [Attorney Advertising](#)

United States: California Delete Act signed into law and introduces single deletion mechanism

12 Oct 2023 • 2 minute read



CPPA

In brief

If you are a data broker or a business that relies on data brokers for targeted advertising, you should be aware that the California **Data Broker Law** will be significantly changed under the **California Delete Act**, which was signed into law by California Governor Newsom on October 10. Under the act, the California Privacy Protection Agency (CPPA) is required to set up, by 1 January 2026, an accessible deletion mechanism where consumers can request deletion via the CPPA that all data brokers then have to honor. Data brokers will have to check the CPPA mechanism to process all deletion requests every 45 days, as well as delete personal information about every California resident who ever made a request through the mechanism every 45 days.

The California Delete Act could profoundly impact how data brokers handle personal information, and subsequently impact the businesses that partner with data brokers for targeted advertising.

registration fee. In registering with the Attorney General, data brokers are required to provide its name, primary physical, email, and internet website addresses.

What the California Delete Act is changing

The California Delete Act will add additional obligations by introducing a single “accessible deletion mechanism”, provided online by the CPPA. Consumers will be able to use such mechanism to request that every data broker that maintains any personal information about the consumer delete such personal information held by the data brokers or associated service providers or contractors. The data brokers will be required to process deletion requests that are made through the CPPA mechanism within 45 days of receiving them, and beginning 1 August 2026, continuously delete the personal information of the requesting consumer and not sell or share new personal information of the consumer. Data brokers will also be required to direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the requesting consumer. This means that California consumers will be able to request deletion of any and all personal information maintained by different data brokers with just a single deletion request.

The act also requires data brokers to provide additional information to the CPPA when registering as data brokers, including to specify whether they collect the personal information of minors, consumers’ precise geolocation, and consumers’ reproductive health care data. Data brokers will also be required to maintain a website free of dark patterns that details how consumers may exercise their privacy rights. Beginning 1 January 2028, and every three years thereafter, data brokers will be required to undergo an audit by an independent third party to determine compliance with the proposed provisions, as well as to submit an audit report to the CPPA upon the CPPA’s written request.

The California Delete Act will also replace the Attorney General with the CPPA as the authority tasked with enforcing the Data Broker Law. The CPPA is the same agency that implements and, together with the California Attorney General, enforces the CCPA.

What this means

Should California consumers extensively use this deletion mechanism, this could reduce the size of a data broker’s database. Partnering businesses that rely heavily on data brokers for their marketing initiatives might feel a ripple effect with less effective targeted advertising.

Looking forward

Data monetization in California faces another blow as data brokers will be subject to additional obligations under the streamlined deletion mechanism for California consumers. The extent of consumer engagement with the mechanism will play a determining role in the impact of the law.

Partner

Palo Alto

[Read my Bio](#)lothar.determann@bakermckenzie.com**Jonathan Tam**

Partner

San Francisco

[Read my Bio](#)jonathan.tam@bakermckenzie.com

Partner

San Francisco

[Read my Bio](#)helena.engfeldt@bakermckenzie.com**Michelle Shin**

Associate

San Francisco

michelle.shin@bakermckenzie.com

Copyright © 2023 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.





05 Jan 2023



[Home](#) > [Data & Technology](#) > [United States: User-enabled privacy controls under CCPA regulations](#)

United States: User-enabled privacy controls under CCPA regulations

04 Jan 2023 • 9 minute read

In brief

Many digital advertising arrangements that companies commonly use may qualify as "selling" or "sharing for cross context behavioral advertising" personal information under the California Consumer Privacy Act (CCPA) in California and laws in a few other US states ([Nevada](#), [Virginia](#), [Colorado](#), [Connecticut](#), [Utah](#)). Businesses state in their online privacy disclosures whether they sold or shared personal information in the last 12 months and whether they will sell or share personal information. Businesses that "sell" or "share" personal information, or use or disclose consumers' sensitive personal information for non-exempt purposes have to treat user-enabled global privacy controls as a valid opt-out request.¹ Internet users can configure their software and devices to send such signals automatically to all websites with a browser plug-in or privacy setting or device setting. Website operators have to implement steps on their end to recognize "global privacy controls" and other signals and satisfy requirements pertaining to opt outs.

Contents

The required steps for recognizing global privacy controls under the CCPA are in flux as the California Privacy Protection Agency is finalizing its regulations (and it remains uncertain if the steps will be the same in Colorado, see 21 December 2022 version of the proposed Colorado Privacy Act Rules [here](#)). Meanwhile, businesses that sell, share, or use or disclose outside of permitted purposes, have to comply with the requirements set forth in the current version of the CCPA regulations concerning the "selling" of personal information.

Compliance with currently operative law and regulations

According to the statutory wording of the CCPA, businesses may elect to either provide opt out links on their webpages or recognize opt-out preference signals.² Nevertheless, under the [currently operative regulations](#), businesses do not enjoy this choice: If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls as a valid opt-out of sales of their personal information for that browser or device, or, if known, the consumer.³ If companies are charged with a violation of the regulations, they may challenge this inconsistency between the statute and regulations in court.

In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices according to the current regulations.⁴ For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, a business shall refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.⁵ That requires businesses to track opt-outs communicated via user enabled privacy controls across the business.

Draft new regulations

The CCPA provides that the California Privacy Protection Agency shall adopt regulations to further the purpose of the CCPA, including issuing regulations for opt-out preference signals.⁶ Any requirements and specifications defined by the agency should, among other things, state that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:

- I. Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.
- II. Choice to "Limit the Use of My Sensitive Personal Information."
- III. Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."⁷

The 2 November 2022 version of the draft regulations includes further requirements related to user enabled privacy controls, and it is again asserted that businesses must honor opt-out signals. While complying with the currently operative law and regulations, business should also consider the following obligations under the new draft regulations:

All opt-out preference signals satisfying certain technical requirements shall be processed. The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

A valid opt-out preference signal shall be treated as a request to opt-out for a browser or device, any associated consumer profile including pseudonymous profiles, and, if known, the consumer. If a consumer uses a browser with an opt-out preference signal enabled, but is not otherwise logged into her account with the business and the business can't otherwise associate her browser with a consumer profile the business maintains, the business shall stop selling and sharing personal information linked to her browser identifier for cross context behavioral advertising, but it would not be able to apply the request to opt-out of the sale/sharing of her account information because the connection between her browser and her account is not known to the business. Conversely, if she is logged in to an account with the business, the business shall honor the opt-out request also with respect to her account and any offline sale or sharing of personal information.

Recognizing opt-out preference signals is in all cases mandatory. Per the draft new regulations, California Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with the regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link. Per the draft new regulations, it does not give a business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if a business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a "non-frictionless" manner.

Businesses that process opt-out preference signals in a frictionless manner, include particular information in their privacy policy, and are able through the signal to fully effectuate a consumer's request to opt out are not required to also post a "Do Not Sell or Share My Personal Information" link. Processing an opt-out preference signal in a frictionless manner means that the business:

- **Shall not** (1) charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal, (2) change the consumer's experience with the product or service offered by the business, or (3) display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal (but displaying if a consumer has opted out is ok)
- **Shall** include in its privacy policy (1) a description of the consumer's right to opt-out of the sale or sharing of their personal information by the business, (2) a statement that the business processes opt-out preference signals in a frictionless manner, (3) information on how consumers can implement opt-out preference signals in a frictionless manner, and (4) instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing
- **Shall** allow the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing

A business that sells consumers' personal information acquired from third parties or offline to marketing partners may not be able to fully effectuate an opt-out request through an opt-out preference signal. The user-enabled signal would be associated only with a consumer's browser or device. The business would not typically know whether it acquires and sells other information about the same consumer, unless the business only sells personal information that it acquires online from the particular consumer. This could be the case for businesses whose only "selling" activities pertain to online digital advertising. Even these businesses may not recognize a consumer who uses their sites with different browsers and devices and enables opt-out signals only on some of them. Most businesses could not apply opt-out requests received via user-enabled browser or device signals to selling or sharing of information they acquired offline or from third parties without additional information on the consumer and the consumer's various browsers and devices. Consumers could provide some of this information by logging into an account, but they cannot be required to do so and few probably would voluntarily provide all information a business would need to identify the consumer across devices, browsers and information acquired offline and from third parties.

Nonetheless, according to the draft new regulations, a business that only sells and shares personal information online for cross-context behavioral advertising purposes may satisfy the requirements for not posting the "Do Not Sell or Share My Personal Information" link.⁸ Such a business gives the consumer using an opt-out preference signal on all devices and browsers an option to fully effectuate their right to opt-out of the sale of sharing of their personal information with user-enabled preference signals.

Industry Concerns

Views on user enabled privacy controls among privacy professionals and industry stakeholders vary. Some flag that the term global privacy control is misleading consumers about what happens when they enable privacy controls.⁹ Businesses will be required to recognize or treat signals in different ways across US states, because definitions and opt-out rights vary, rendering operationalizing the response process even more burdensome.

Alternatives

Businesses that do not take steps to recognize user-enabled opt-out signals have to stop disclosing personal information in ways that qualify as "selling" or "sharing" of personal information. One option is to require all vendors to sign contracts that qualify them as service providers under CCPA. But, this option does not allow businesses to work with vendors for cross-context behavioral advertising purposes, because this is not a permitted business purpose for service providers under CCPA.¹⁰ Another option is to seek directions to disclose personal information from users, for example, with a pop-up banner, because this will also negate "selling" and "sharing" under CCPA.¹¹ In its draft regulations, the California Privacy Protection Agency clarifies that banners seeking affirmative acceptance of web cookies are not suited to meet requirements to enable opt-out requests under CCPA, because cookies concern the collection of personal information and not the sale or sharing of personal information.¹²

1. CCPA Regulations §999.315(c) from the Cal. Attorney General and draft CCPA regulations 7026(a)(1) of the draft CCPA regulations from the California Privacy Protection Agency.

2. Per Cal. Civ. Code §1798.135(b)(3), "a business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect to comply with subdivision (a) or subdivision (b)". The reference to "subdivisions (a) or (b)" seem intended to refer to §1798.135(a) or §1798.135(b)

3. CCPA Regulations §999.315(c). And the draft CCPA regulations specify in §7025 that recognizing opt-out preference signals is in all cases mandatory.

4. CCPA Regulations §999.315(d).

5. Cal. Civ. Code §1798.135(c)(4).

6. Cal. Civ. Code §1798.185 (a) (19), and §1798.199.40(b).

7. Cal. Civ. Code §1798.185 (a) (19) (A). This mandated choice language is different from the language mandated to be included on opt-out links provided by a business of "Do Not Sell or Share My Personal Information" per Cal. Civ. Code §1798.135(a)(1).

8. §7027(g)(3)(B) of draft regulations.

9. See, for example, [When a "Global Privacy Control" really isn't](#).

10. According to Cal. Civ. Code §1798.140 (ad) and (ah), disclosures of personal information to third parties qualify as "selling" or "sharing" unless certain limited exceptions apply. Under Cal. Civ. Code §1798.140(ai)(2), a service provider is not a third party. Under Cal. Civ. Code §1798.140(ag)(1), companies must use personal information only for business purposes recognized by CCPA to qualify as a "service provider" and avoid qualifying as a "third party." Under Cal. Civ. Code §1798.140(3)(6), cross-context behavioral advertising is not a "business purpose." Therefore, companies that receive personal information for purposes of cross-context behavioral advertising are not recognized as "service providers" and the businesses that provide personal information to them are typically considered to be "selling" and "sharing" personal information.

11. According to Cal. Civ. Code §1798.140 (ad)(2)(A)(i) and (ah)(2)(A).

12. Draft regulations §7026(a)(4) and 7027(b)(4).

Contact Information

Lothar Determann

Partner

Palo Alto

[Read my Bio](#)

lothar.determann@bakermckenzie.com

Helena Engfeldt

Partner

San Francisco

[Read my Bio](#)

helena.engfeldt@bakermckenzie.com

Copyright © 2022 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.

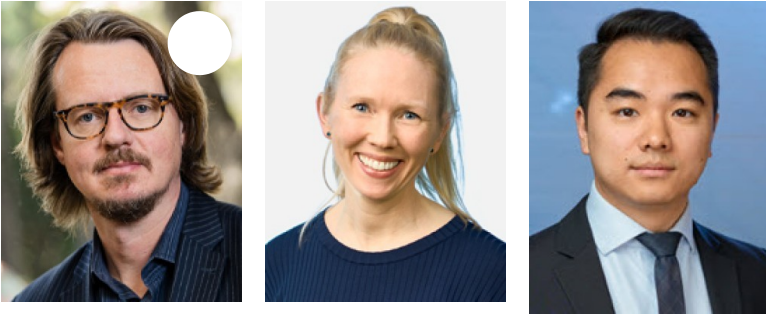
The Employer Report

NAVIGATING US AND GLOBAL EMPLOYMENT LAW

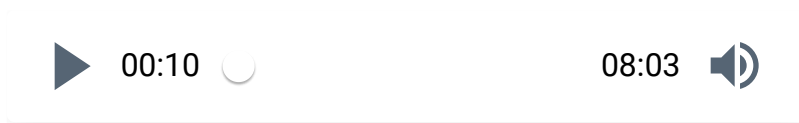
Looking ahead to 2024: California privacy law action items for employers



[Tim Mossholder](#), Unsplash



By Lothar Determann, Helena Engfeldt & Jonathan Tam on December 14, 2023



On January 1, 2024, businesses must post updated Privacy Policies under the California Consumer Privacy Act (CCPA), which requires annual updates of disclosures and fully applies in the job applicant and employment context since January 1, 2023.

With respect to **job applicants** and **employees**, businesses subject to the CCPA are required to:

1. Issue detailed privacy notices with prescribed disclosures, terminology, and organization;
2. Respond to data subject requests from employees and job candidates for copies of information about them, correction, and deletion;
3. Offer opt-out rights regarding disclosures of information to service providers, vendors, or others, except to the extent they implement qualified agreements that contain particularly prescribed clauses; and
4. Offer opt-out rights regarding the use of sensitive information except to the extent they have determined they use sensitive personal information only within the scope of statutory exceptions.

If employers sell, share for cross-context behavioral advertising, or use or disclose sensitive personal information outside of limited purposes, numerous additional compliance obligations apply. For more: see also our related previous post: [Employers Must Prepare Now for New California Employee Privacy Rights](#).

Key recommendations to heed now

- **Review contracts with parties to whom you disclose personal information about applicants and personnel.** The CCPA prescribes certain types of clauses that have to appear in agreements between parties exchanging personal information, and you will have to include

certain data processing clauses if you do not want to be considered to be “selling” (which the CCPA defines to mean disclosing in exchange for monetary or valuable consideration) or “sharing” (which the CCPA defines to mean disclosing for the purposes of cross-context behavioral advertising) personal information and offer related opt-out processes. It is not practical for employers to offer opt-out rights in most scenarios, due to the CCPA’s non-discrimination requirements. The [CCPA regulations](#), which are currently being revised by the California Privacy Protection Agency (latest as of this publication is available [here](#)), include additional requirements. Businesses should continue to update such contracts with parties it discloses personal information to.

- **Prepare/revise notices at collection and include HR data in your online CCPA Privacy Policy.** As collection notices in the employment context have been required under the CCPA since 2020, but new specific disclosure requirements apply since January 1, 2023. Your comprehensive online CCPA privacy policy will also have to reflect your processing of HR data. You should consider updating/preparing a privacy notice at collection that is specific to the CCPA and separate from any privacy notice you might use to address privacy laws in other jurisdictions, since California laws establish increasingly unique requirements and use unique terms that may be difficult to reconcile with those of other jurisdictions (since January 1, 2023, businesses must use specific terms from the CCPA to describe categories of personal information in all “notices at collection,” including context-specific, real-time notices about specific data processing activities, such as security cameras, computer monitoring, and job application processes). At the same time, you have to be mindful of setting or negating privacy expectations. If you issue privacy notices to job applicants and personnel that merely address CCPA disclosure requirements, the recipients of such notices may develop privacy expectations that could later hinder you in conducting investigations or deploying monitoring technologies intended to protect data security, co-workers, trade secrets and compliance objectives.
- **Prepare/update and document your data subject request program and train HR professionals.** Your job applicants and personnel who reside in California have gained data access, portability, correction, deletion and other rights in 2023. You should implement protocols and training to ensure that your HR, compliance and similar teams can deal with their requests in a consistent, timely and compliant manner. Any email, spreadsheet, contract or other document that refers to a California-based employee constitutes their “personal information” which you may have to produce in response to an access request, free of charge. To keep track of where information is stored while reducing the amount of data potentially subject to data access requests, you should work on tightening your data retention and deletion protocols. This will also help you comply with CCPA’s new data minimization requirements. Documenting your program is important because the draft regulations also define the concept of “disproportionate effort” within the context of a business responding to

a consumer request. Disproportionate effort is defined as the time and/or resources expended by a business to respond to an individualized request significantly outweighing the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances. Under the draft regulations, a business can only claim disproportionate effort as an exemption to the duty to respond to a data subject request if they have in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and its regulations. The draft regulations give examples of circumstances that may amount to disproportionate effort and businesses should consider as part of the fact-gathering involved in preparing required privacy notices to also document when it would amount to a disproportionate effort to identify particular information in response to a data subject request and why.

- **Consider whether and the extent to which you process “sensitive personal information,” such as if you use employee monitoring software, and address related CCPA requirements.** California residents will have the right to request that businesses stop using and disclosing their “sensitive personal information” outside of specific purposes. CCPA defines “sensitive personal information” to include, among other things, government identifiers, precise geolocation data, information on racial or ethnic origin, religious or philosophical beliefs, and the contents of a California resident’s mail, email and text messages addressed to someone other than the business. If you process sensitive personal information outside of the specific purposes, you have to post a link titled “Limit the Use of my Sensitive Personal Information” online. CCPA may also require you to engage in privacy risk assessments and allow California residents to opt-out of automated decision-making activities in certain situations. Diversity and Inclusion data often contains sensitive personal information and employers should consider if they run programs that could trigger rights to limit use or disclosure of such information (see our thoughts on [Running a privacy compliant inclusion and diversity program globally](#)). The California Privacy Protection Agency has clarified and expanded some of these requirements in prescriptive and wordy regulations that the agency enacted in March 2023 and will start enforcing in March 2024 (after a court prohibited earlier enforcement as the authority had planned). Meanwhile, the California Attorney General, who also enforces CCPA in parallel, [announced an initiative in July 2023](#) to demand information from employers regarding their compliance measures concerning CCPA. Visit our [California privacy law blog](#) for our take on developments.

Enforcement

Both the California Attorney General’s Office and the California Privacy Protection Agency enforce the CCPA. The authorities can investigate violations, hold hearings, issue cease-and-desist orders,

and impose administrative fines of up to USD 7,500 for each intentional violation. Businesses no longer enjoy a 30-day cure period. Sign up for our [Privacy Webinar Series](#) for more information.



The Employer Report



Copyright © 2023, Baker & McKenzie LLP. All Rights Reserved.



DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: TRADE-OFFS



BY
LOTHAR DETERMANN



&
TEISHA JOHNSON

The authors are partners at Baker McKenzie's Palo Alto and Washington D.C.'s offices. Opinions expressed in this article are solely their own and not their firm's, clients' or others.

CPI TECHREG TALKS...
...with Samuel A.A. Levine



DATA BROKERS IN THE HOT SEAT: A CONTINUING STORY
By Jessica L. Rich



TO SHARE OR NOT TO SHARE: REGULATING DATA BROKERS
By Jeanne Mouton & Christian Rusche



DATA BROKERS: INTERMEDIARIES FOR MORE EFFICIENT DATA MARKETS?
By Andreas Schauer & Daniel Schnurr



DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: TRADE-OFFS
By Lothar Determann & Teisha Johnson



IS PERSONAL DATA STILL UP FOR GRABS?
By Adriana Hernandez Perez



KEEPING UP WITH THE ALCHEMISTS - REGULATING DATA BROKERS IN AUSTRALIA
By Chandni Gupta



Visit www.competitionpolicyinternational.com for access to these articles and more!

DATA BROKER REGULATION - COMPETITION v. PRIVACY CONSIDERATIONS: TRADE-OFFS By Lothar Determann & Teisha Johnson

In the ongoing debate concerning data broker regulation, tradeoffs between competition and privacy are not always holistically appreciated. This article examines the importance of data protection for individual privacy and access to data for competition, discusses the role of data brokers as to data privacy and sharing, and then reviews existing, new, and proposed regulations of data brokers. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from increased fraud, reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.



01

INTRODUCTION

Data brokers face stiff criticism, lawsuits, actions from regulators, proposed new legislation and regulation, and political headwinds, in the United States as elsewhere.² Privacy advocates and journalists claim data brokers are not sufficiently regulated,³ even though data brokers have been subject to privacy law restrictions in some of the oldest U.S. privacy laws. In the ongoing debate, tradeoffs between competition and privacy are not always holistically appreciated.

02

DATA

In an increasingly interconnected world, data is a valuable asset. No one owns data,⁴ yet every business needs information to make intelligent decisions about market focus, product development, pricing, advertising, and all other aspects of running a successful company. Every online action — from liking a social media post to buying a new shirt — generates data. Companies that operate successful online presences collect lots of information that they can use to compete in their core business areas, monetize to target advertisements on their platforms, or sell to other companies or government agencies.⁵ Many new market entrants and smaller businesses in particular state that they need to purchase data to compete.

² See, for example, www.cnn.com/2023/08/15/tech/privacy-rules-data-brokers/index.html.

³ See, for example, www.popsoci.com/technology/data-brokers-explained/.

⁴ Lothar Determann, No One Owns Data, 70 Hastings Law Journal 1 (2019), available at SSRN: <https://ssrn.com/abstract=3123957>.

⁵ See, www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.

⁶ See, recital (d) of Assembly Bill 1202 that introduced registration requirements for data brokers in California, see <https://legiscan.com/CA/text/AB1202/2019>.

⁷ Cal. Civ. Code §1798.99.80(d).

03

BROKERS

Generally, brokers act as intermediaries between buyers and sellers of any item of value, including real estate, commodities, securities, and all kinds of products and services. Brokers focus on meeting demand and help optimize market dynamics, pricing, and quality. They play an important role for commerce and competition in all areas. So do data brokers. “Data brokers may provide information that can be beneficial to services that are offered in the modern economy, including credit reporting, background checks, government services, risk mitigation and fraud detection, banking, insurance, and ancestry research, as well as helping to make determinations about whether to provide these services.”⁶

04

PRIVACY CONSIDERATIONS

Data brokers sell various categories of data and not all relates to individual persons. But, much of the information humans care about relates to humans and thus qualifies as “personal information” or “personal data.” Under California privacy law, “data broker” means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.⁷ Without a direct relationship, data brokers cannot easily inform consumers about their data collection and processing practices. From the consumer’s perspective, the brokers operate “behind the scenes,” collecting information from numerous sources, including e-commerce websites, social medial platforms, public records, online transactions, surveys, and more. These data collection efforts enable data brokers to amass a wide array of data and information, from basic personal details (e.g. names, addresses, phone numbers, email addresses) to intricate personal behavior insights (e.g. financial status, family connections, health conditions, details on shopping and online browsing activities, travel habits, and ge-

olocation data) that can create a detailed profile of an individual. The collected data can also be aggregated and compiled into comprehensive datasets to be licensed or sold to various businesses and institutions including, advertisers, marketers, researchers, and financial institutions. The businesses that ultimately buy and use personal information about consumers often do not have relationships with the consumer either and with some of them -- e.g. collection agencies, law enforcement authorities, and telemarketers -- consumers would rather not have relationships at all. Most consumers would prefer that their data is not sold to organizations that do not wish them well or might harass them with cold calls and unwanted text messages. Most consumers also do not see any tangible upside from their data being traded by brokers. Many fear that poor data quality or hostile data usage practices could ultimately harm them. Some feel they should receive a “cut” from the profits generated with their data.⁸

05 COMPETITION CONSIDERATIONS

Without data, companies cannot effectively develop products, stock the right amount of goods in the right place, target advertisements effectively to potentially interested persons, or make informed decisions about important issues such as loans and payment terms. As the significance of data continues to increase, firms without sufficient access to data, such as new market entrants and smaller players, may not be able to effectively compete with larger, already established firms. Data brokers can play an important role in our data-driven economy by providing entities with valuable consumer insights through data selling and sharing.

However, data collection and sale can also create competition concerns if data brokers amass large amounts of unique data resulting in a data broker gaining significant market power. If access to that data set is withheld (either entirely or selectively) or if the cost of obtaining the data is so large that only a limited number of well-established data purchasers can financially purchase the data, this could create barriers to entry both for smaller firms desiring to purchase the data and for smaller data brokers attempting to enter the market

8 <https://www.cnn.com/2019/02/12/california-gov-newsom-calls-for-new-data-dividend-for-consumers.html>.

9 15 U.S.C. §§ 1681–1681x. On the history of credit bureaus and regulation, see Rowena Olegario, Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development, <http://documents.worldbank.org/curated/en/209261468762614853/Credit-reporting-agencies-their-historical-roots-current-status-and-role-in-market-development>.

10 See 16 C.F.R. Part 682.

as a data broker. Owning large amounts of data—particularly unique data—heightens the competition concern as there is an increased risk of the data owner taking actions to solidify its market position by behaving in anticompetitive ways that could slow innovation, cause prices to rise, reduce quality and choice, and cause other negative effects such as affecting credit decisions and how customers are treated.

Data brokers can also enhance the competitive environment and facilitate positive outcomes for consumers by embracing and facilitating the flow of data. Consumers can directly benefit from data trading where companies offer services or financial incentives to consumers in exchange for collecting information from consumers. Also, consumers can indirectly benefit, namely from effective competition, informed product development, relevant advertisements, and loan risk mitigation throughout the economy. If overly rigid data broker regulation inhibits data selling and sharing, smaller and newer companies may not have access to sufficient data to enter new product markets and compete. Without competition, companies could then solidify their market positions and raise prices, slow down innovation, deteriorate products, withhold credit, and treat consumers poorly.

06 DATA BROKER LAWS AND REGULATIONS

Fair Credit Reporting Act. Data brokers have been subject to sector-specific data privacy laws for more than 50 years in the United States. Congress enacted one of the oldest data privacy laws in the world, the federal Fair Credit Reporting Act (“FCRA”), in 1970 to regulate credit reporting agencies and provide privacy rights for personal data in consumer reports.⁹ FCRA was substantially updated by the Fair and Accurate Credit Transactions Act (“FACTA”) in 2003.¹⁰ Companies have to comply with FCRA if and to the extent they act as “consumer reporting agencies,” “users” or “furnishers.” Most companies act at a minimum as “users” of credit reports, namely when they obtain background checks on employees or candidates. A “consumer reporting agency” is any person or entity that compiles or evaluates information on consumers for the purpose of furnishing consumer reports

to third parties for a fee.¹¹ Equifax, Experian, and TransUnion are among the most prominent consumer reporting agencies. Other businesses that collect similar data on consumers may also be subject to the FCRA rules, depending on the purposes for which the data they sell is used.¹² “Users” are employers, lenders, insurers, and other companies that use consumer reports for various purposes.¹³ “Furnishers” are companies that report information about transactions with consumers to consumer reporting agencies, such as banks or merchants that report that a debtor is late making payments. A company that furnishes only reports regarding its own transactions does not become a “consumer reporting agency,” because such reports are excluded from the definition of “consumer report.”¹⁴ Friends, acquaintances and neighbors who answer requests for information from consumer reporting agencies do not qualify as furnishers either.¹⁵

State Privacy Laws. In 1975, California enacted the California Consumer Credit Reporting Agencies Act (“CCRAA”), with a similar focus as the federal FCRA.¹⁶ The CCRAA regulates consumer credit reporting agencies doing business in California. More recently, states including California, Texas, Vermont, and Oregon enacted laws regulating data brokers more broadly. Vermont was the first state to require data brokers to register with the state government. California soon followed, and just this year Texas and Oregon joined California and Vermont in enacting laws regulating data brokers. The specific requirements and obligations imposed on data brokers vary by state. However, there are common themes in the regulations, including: (1) similarities in the definition of “data broker” and “personal data;” (2) the requirement that data brokers register in the state; and (3) penalties associated for data brokers who fail to register and/or provide the required information to the state. State rules also require that data brokers maintain certain security measures with respect to the data.

11 15 U.S.C. § 1681a(f).

12 LinkedIn was sued in a class action over alleged FCRA violations, but the suit was dismissed, see *Sweet v. LinkedIn Corp.*, N.D. Cal., No. 5:14-cv-04531-PSG, 2015 WL 1744254 (N.D. Cal. April 4, 2014). Spokeo settled with the FTC on alleged FCRA violations, Stipulation for Entry of Consent Decree and Order for Civil Penalties, Injunction and Other Relief, *United States of America v. Spokeo, Inc.*, No. CV12-05001 (C.D. Cal. June 7, 2012), available at www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeoorder.pdf.

13 See 15 U.S.C. § 1681m (requirements on users of consumer reports); 15 U.S.C. § 1681s-2 (responsibilities of furnishers of information to consumer reporting agencies).

14 15 U.S.C. § 1681a(d)(2)(A)(i).

15 16 C.F.R. § 660.2(c).

16 Cal. Civ. Code §§ 1785.1-1785.36. The law became effective in California in 1975 and has been subject to several amendments. See, for example, www.leginfo.ca.gov/pub/09-10/bill/sen/sb_0901-0950/sb_909_cfa_20100621_110753_asm_comm.html.

17 9 V.S.A. §§ 2430, 2433, 2446 and 2447

18 See, Guidance on Vermont’s Act 171 of 2018 Data Broker Regulation, [2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf](https://www.vermont.gov/files/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf) (vermont.gov).

19 9 V.S.A. § 2430(4)(A).

20 9 V.S.A. § 2430(1)(A).

21 9 V.S.A. § 2446 (b).

A. Overview of State Data Regulation Rules

Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers.¹⁷ Vermont’s law established registration, disclosure and data security requirements for data brokers trading in Vermont residents’ personal information. Data brokers must register annually and adopt information security programs with appropriate safeguards to protect personal information.¹⁸ The Vermont law defines data brokers to mean a business that “knowingly collects and sells or licenses to third parties brokered personal information of a consumer with whom the business does not have a direct relationship,”¹⁹ and defines brokered personal information as “computerized data elements, if categorized or organized for dissemination to third parties” that include certain items about a Vermont consumer, including name, address, date or place of birth, mother’s maiden name, biometric data, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information would reasonably allow the consumer’s identification with reasonable certainty.²⁰ The law imposes civil penalties of up to \$50/day (not exceeding \$10,000 per year) for data brokers that fail to register.²¹ As Vermont was the first state to enact data broker laws, it set a precedent which other states have followed.

“Vermont, in 2018, became the first state to enact a law implementing registration requirements and regulations with respect to data brokers”

California enacted a data broker law that looked similar (but not identical) to Vermont’s data broker law. The California law requires data brokers to register every year on or before January 31 with the California Attorney General, and pay an annual registration fee.²² In registering with the Attorney General, data brokers are required to provide its name, primary physical, email, and internet website addresses. California’s data broker law borrowed many of the broad definitions from the previously adopted California Consumer Privacy Act (“CCPA”) enacted in 2018, including “business,” “consumer,” “personal information” and “sale.”²³ Companies that exchange employee or business contact information with affiliates or other business partners for consideration (monetary or other) may qualify as a business that sells personal information under CCPA; if a business does not have a direct relationship with the consumer to whom the data relates, the business may have to register as a data broker.

In September 2023, California amended its data broker law, and passed Senate Bill 362 adding additional obligations on data brokers by introducing a single “accessible deletion mechanism.”²⁴ California consumers will be able to use the mechanism via a website maintained by the California government to request that every data broker that maintains any personal information about the consumer delete such personal information held by the data brokers or associated service providers or contractors.²⁵ The data brokers will be required to process deletion requests that are made through the CPPA mechanism within 31 days of receiving them, and in 2026, continuously delete the personal information of the requesting consumer and not sell or share new personal information of the consumer. Data brokers will also be required to direct all service providers or contractors associated with the data broker to delete all personal information in their possession related to the requesting consumer. The new law will require data brokers to provide additional information when registering as data brokers, including specifying whether they collect the personal information of minors, consumers’ precise geolocation, and consumers’ reproductive health care data.

Currently, the new California law is the first and only law giving consumers the ability to request that their data be

deleted in a single request. Also, California applies the most rigid restrictions on “selling” and “sharing” of personal information in the United States and probably worldwide, applicable to businesses that have a direct relationship with consumers and who supply data to brokers and other businesses.²⁶ These restrictions could significantly reduce the amount of California consumer information that data brokers can trade, unless data brokers and businesses can make the case to consumers that consumers benefit from more efficient competition enabled by data trading. California privacy law also requires companies to inform consumers about the value of their personal information to the business in “notices of financial incentives” whose disclosures and terminology is dictated by prescriptive statutory requirements and regulations.²⁷ It remains to be seen whether these restrictions and transparency requirements will enable and enhance fair competition in data markets or stifle the data broker industry so much that smaller businesses can no longer compete with large data owners, which do not have to sell or share data.

“Currently, the new California law is the first and only law giving consumers the ability to request that their data be deleted in a single request”

In June, Texas signed into law a new data broker law (SB 2105) (effective as of September 1, 2023) creating registration, security, and disclosure requirements for data brokers that meet certain annual revenue or processing thresholds regarding personal data (any information that links or is reasonably able to be linked to an individual, including pseudonymous data used in combination with other identifying information).²⁸ Texas considers a data broker to be any business entity whose principal source of

revenue is derived from collecting, processing or transferring personal data that the entity did not collect directly from the individual linked to the data.²⁹ Data brokers operating in Texas are required to (1) pay a fee and register with the state, (2) post language on its website or app identifying itself as a data broker, and (3) implement and maintain a comprehensive written information security program.³⁰ The law also outlines what must be included in the security program, including identifying risks, employee training policies, monitoring plan performance, and implementing technical safeguards around data. Violations of the law are subject to penalties of at least \$100 per day, not to exceed \$10,000 in one year.³¹

Oregon is the most recent state to pass a data broker registration law (HB 2052). The law was enacted in late July 2023, and similar to Vermont, California, and Texas, requires data brokers to pay a fee and register with the Oregon Department of Consumer and Business Services.³² Oregon defines data brokers as a business entity or part of a business entity that collects and sells or licenses “brokered personal data” to another person, and broadly defines “brokered personal data” as any computerized data elements about an Oregon resident if those elements are categorized or organized for the sale of licensing to another person.³³ This includes basic information about an individual, such as name, addresses, birthdate or place, biometric information, social security number (or any government-issued identification number) and any other information that alone or in combination with other licensed/sold information that can be reasonably associated with an Oregon resident.³⁴ Data brokers that violate the broker registration law may face penalties up to \$500 for each violation, each day (with a yearly cap of \$10,000). HB2052 is set to go into effect Jan. 1, 2024.³⁵

Though each state has slightly different rules, each state defines “data broker” and “personal data” broadly, requires data brokers to register, and have similar penalties for violations. While the similarities in state regulations could conceivably provide a roadmap to federal regulation, it is also possible that U.S. federal regulation of data brokers will go

beyond what the states have implemented and further burden the industry with additional complexities if federal law does not preempt state laws.

B. Role of the U.S. Federal Agencies

Congress and federal agencies are becoming increasingly bullish on data broker regulation. While this is not new –there have been proposed Congressional bills and statements by federal agencies regarding data brokers over the years--the Consumer Financial Protection Bureau (“CFPB”) recently announced that it plans to propose rules under the Fair Credit Reporting Act (“FCRA”) requiring data brokers to comply with the FCRA.³⁶ The FCRA establishes data privacy requirements when consumer reporting agencies use consumer data for items such as credit and employment. The stated purpose of the to-be-proposed rules is to protect American consumers from data brokers by subjecting data brokers to greater oversight and regulation, ensuring that sensitive consumer data is protected, and preventing misuse and abuse by data brokers.

“Though each state has slightly different rules, each state defines “data broker” and “personal data” broadly, requires data brokers to register, and have similar penalties for violations”

In order to require data brokers comply with the FCRA, according to CFPB Director Rohit Chopra, the CFPB is considering categorizing a data broker that sells certain types of consumer data, such as a consumer’s payment history, income, and criminal records as a “consumer reporting agency,” thus triggering requirements to ensure

22 Cal. Civ. Code §1798.99.82.

23 See, Determann, California Privacy Law, Practical Guide and Commentary, Chapter 2C (5th Ed. 2023).

24 Cal. SB 362 (2023)

25 https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/united-states-senate-bill-362-to-amend-california-data-broker-law.

26 Lothar Determann, California Privacy Law Vectors for Data Disclosures, in: *Data Disclosure: Global Developments and Perspectives*, edited by Moritz Hennemann, Kai von Lewinski, Daniela Wawra and Thomas Widjaja, Berlin, Boston: De Gruyter, 2023, pp. 121-146, <https://ssrn.com/abstract=4146903>.

27 <https://www.connectontech.com/united-states-california-attorney-general-sets-sights-on-consumer-loyalty-programs-for-ccpa-enforcement/>.

28 See Texas S.B. No. 2105 (2023).

29 See Texas S.B. No. 2105, Sec. 509.001 (2023).

30 See Texas S.B. No. 2105 (2023)

31 See Texas S.B. No. 2105, Sec. 509.008 (2023).

32 See Oregon H.B. 2052 (2023).

33 Oregon H.B. 2052, Section 1 (2023).

34 See Oregon H.B. 2052, Section 1 (2023).

35 Oregon H.B. 2052, Section 1, 7 (2023).

36 See [Protecting the Public from Data Brokers in the Surveillance Industry](#), August 2023

that the data sold is accurate, prohibits misuse, and contains a mechanism to handle inaccurate information.³⁷ The rationale behind treating data brokers selling those types of consumer data as a consumer reporting agency centers around how that data is used. According to the CFPB, this type of data is typically used for credit and employment determinations, and thus should comply with the FCRA.

The CFPB and Director Chopra noted that the CFPB's rulemaking will complement other federal agencies, specifically recognizing the role of the Federal Trade Commission (FTC) as leading many efforts on privacy and data security.

The FTC has been actively involved in evaluating the conduct of data brokers for over a decade.³⁸ As the federal commission tasked with overseeing consumer protection, the FTC's primary concerns regarding data brokers have centered around data security, transparency, and misuse of personal information. In 2012, the FTC issued **Orders** requiring nine data brokerage companies to provide the agency with information about how they collect and use consumer data, specifically with respect to privacy practices.³⁹ That same year, they also **called** on the data broker industry to improve business practices by increasing transparency.⁴⁰ The FTC has continued to devote resources to gathering information about data brokers, monitoring data broker practices, and has filed suit against companies for alleged violations of the FTC Act⁴¹ and the FCRA. The FTC views the collection, use and sale of consumer data as having the potential to cause harm to consumers due to the sensitive nature of the information collected, possible lack of protection of such data, and the potential for misuse.

The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act. The FTC has used this authority to take action against various data brokers for violations of the FTC Act consumer protection

laws. The cases have resulted in significant settlements requiring data brokers to pay fines, institute tighter security measures, provide clearer disclosures to consumers, or cease operations entirely. In 2014, the FTC filed suit and agreed to settle with two data brokers on violations of the FCRA and FTC Act.⁴² The allegations revolved around the use of consumer data without notifying consumers that their information was being reported, and without ensuring accuracy.⁴³ The FTC also published an extensive report calling for transparency and accountability for data brokers.⁴⁴ In this report, the Commission recommended that Congress consider enacting legislation to regulate data broker practices, and allow consumers to have more rights and access to their data. The key findings in the report emphasized the limited control consumers have over their personal data. The collection of data, often without consumer knowledge, can flow through multiple layers of data brokers, allowing data to be exchanged between brokers, and leading to multiple levels of data brokers storing, accessing, and making inferences about consumers based on this data.⁴⁵ All harms that the FTC would like to protect against.

“The FTC Act, which prohibits deceptive and unfair practices, gives the FTC the authority to initiate enforcement actions or perceived violations of the FTC Act

While Congress has not enacted legislation based on the FTC's recommendation, the FTC continues its pursuit against alleged consumer harms caused by data brokers. In 2016, the FTC issued an **Order** settling charges against a data broker operation who was alleged to have fraudu-

lently collected and sold consumer data without their consent, in violation of the FTC Act, resulting in a \$7 million harm.⁴⁶

In the past year, the agency has reconfirmed its commitment to protecting sensitive consumer data, including geolocation and health data, promising that protecting consumer data is a top priority.⁴⁷ The FTC also warned that they are committed to using the “full scope” of their authority to enforce the law against illegal use and sharing of highly sensitive data.⁴⁸ To emphasize the point, the FTC filed a complaint alleging that a location data broker engaged in unfair or deceptive acts in violation of the FTC Act when it acquired consumer's geolocations data and utilized this data to track consumer's movements and locations.⁴⁹ The complaint alleged the data broker sold precise geolocation data associated with unique identifiers revealing consumers visits to sensitive locations, and that the data broker employed “no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations.”⁵⁰ The lawsuit claimed the sale of the highly sensitive data put consumers at significant risk and would likely cause substantial injury. The FTC sought to stop the sale of the sensitive geolocation data by permanently barring the data broker from selling consumer data in the future and requiring the company to delete the data it has collected. The case was dismissed, ordering that while the FTC's legal theory of consumer injury was plausible, the FTC had not made sufficient factual allegations to proceed. To do so, it must not only claim that the practices could lead to consumer injury, but that they are likely to do so.⁵¹ In response, the FTC filed an amended complaint that currently is under seal.

The setback has not deterred the FTC from staying at the forefront of the data broker regulation efforts. The agency has shown that it will not hesitate to go after companies for alleged misuse of consumer data, including the collection, retention, and exchange or sale of this sensitive data. To accentuate the point, in late September, 2023, speaking at the 2023 Consumer Data Industry Association Law & Industry Conference, the Director of the FTC's Bureau of Consumer Protection voiced his concern with data brokers looking to “maximize” data at the cost of the consumer, posing serious risks.⁵²

It is clear that there will continue to be scrutiny and enforcement around data brokers. Though the federal landscape lacks a comprehensive regulatory framework, the FTC has become the federal agency leading the charge against alleged violations by data brokers, and individual states have taken the initiative to introduce and pass legislation regulating data brokers.. As the economy evolves and data becomes an even more invaluable commodity, we can expect to see new state and federal laws regulating data brokers.

“It is clear that there will continue to be scrutiny and enforcement around data brokers

37 See [Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices](#), August 2023.

38 See [Data Brokers: A Call for Transparency and Accountability, 2014](#); and [FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information | Federal Trade Commission](#).

39 See [Order to File Special Report](#).

40 See [FTC Report, Protecting Consumer Privacy in an Era of Rapid Change](#), March 2012.

41 15 U.S.C. §§ 45(a) et. al.

42 See [Consent, U.S. v. Instant Checkmate, Inc.](#); and see, [U.S. v. Infotrack Information Services, Inc.](#)

43 See [Complaint, U.S. v. Infotrack Information Services, Inc. \(2014\)](#).

44 See [Data Brokers, A Call for Transparency and Accountability](#), FTC, May 2014.

45 See [Data Brokers, A Call for Transparency and Accountability](#), FTC, May 2014.

46 See [Stipulated Order, FTC v. Sequoia One, LLC \(Nov. 2016\)](#)

47 <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>.

48 <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>.

49 [FTC v. Kochava Inc., Case No. 2:22-cv-00377 \(Complaint\)](#).

50 [FTC v. Kochava Inc., Case No. 2:22-cv-00377 \(Complaint\)](#).

51 See, [FTC v. Kochava Inc., Case No. 2:22-cv-00377 \(Memorandum Decision and Order\)](#), May 24, 2023

52 https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

07

CONCLUSIONS AND OUTLOOK

Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs. Consumers may benefit from added privacy protections if the new laws and regulatory actions enhance data accuracy, the quality of disclosures, transparency, and fair information processing practices. But, consumers may suffer from reduced competition, fewer charge-free information services, price increases, and stifled innovation if additional regulations result in reduced competition, data sharing, and information availability. Established businesses with large amounts of data do not have to sell or share their information and could rely less on data purchases. Similarly, data brokers that amass large amounts of unique data can pick winners and losers if they decide to whom they will and will not sell their data. Legislators will need to be thoughtful about data broker regulations—if regulation creates barriers to easy entry, it can put smaller players at a competitive disadvantage, resulting in data being consolidated into the hands of few. Smart, balanced regulations can create an environment where data brokers have a positive impact on the competitive marketplace. As regulators continue to evaluate the impact of data brokering on both privacy and competition, this discourse will continue to evolve. ■

“

Data brokers face additional and varying restrictions in state and federal privacy and consumer protection laws that will increase their compliance costs

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit [competitionpolicyinternational.com](https://www.competitionpolicyinternational.com) today to see our available plans and join CPI's global community of antitrust experts.



Lothar Determann

California Privacy Law Vectors for Data Disclosures

A	Data Monetization Trends and Consumer Information Requirements in California	124
B	Privacy and Data Protection Legislation	128
	I Privacy	129
	II Privacy Law and Data Processing Regulation	131
	1 Constitutional Safeguards	132
	2 International Treaties	132
	3 Statutes	133
	III Policy Reasons for Privacy Protections and Limitations	133
C	Legislative Approaches	135
	I Privacy Protection	135
	II Data Protection	135
	III Information Access Blocking Prohibitions	136
	IV Data Security Laws	138
	V Trade Secret Laws	138
	VI Data Ownership	138
	VII Freedom of Speech and Information	139
	VIII Data Residency and Retention Requirements	139
D	International Privacy Law at Crossroads	140
	I Privacy v. Data Protection	140
	II Adequacy of EU Regulations of Data Processing	141
	III Why Then Follow Europe?	142
E	Conclusion and Outlook	144

Lothar Determann teaches computer, internet and data privacy law at the Free University of Berlin, University of California, Berkeley School of Law and Hastings College of the Law, San Francisco, and he practices technology law as a partner at Baker McKenzie LLP in Palo Alto. This contribution reflects views the author shared in presentations at the Conference on ‘Vectors of Data Disclosure’ hosted by the Bavarian Institute for Digital Transformation in Munich in June 2022, <www.bidt.digital/event/conference-vectors-of-data-disclosure/> and at the US Federal Trade Commission privacy hearings in April 2019 and contains excerpts of prior articles, including Lothar Determann, ‘Data Privacy and Data Security Legislation: Policy focus on data processing regulation v. specific individual harms’ in David A. Marcello (ed), *International Legislative Drafting Guidebook: 25th Anniversary Celebration* (Carolina Academic Press 2020) 189; Lothar Determann, ‘Privacy and Data Protection’ (2019) 1 *Moscow Journal of International Law* 18; Lothar Determann, ‘La normativa de protección de datos en la encrucijada’ [Data Privacy Legislation at Crossroads] (2019) *almacen de derecho* <<https://almacenderecho.org/la-normativa-de-proteccion-de-datos-en-la-encrucijada>> accessed 07.02.2023.

At the conference on ‘Vectors of Data Disclosure’ in June 2022, scholars from several disciplines came together to examine when and why persons or organizations share information. This depends on numerous vectors, ie, directional forces¹ that drive if, when, where, to whom and under what conditions data is disclosed. Humans disclose personal information about themselves based on individual inclinations, socialization, cultural norms, power dynamics, technological necessities and economic considerations, such as perceived benefits.

Lawmakers also provide vectors for data disclosures, directly and indirectly. For example, under tax laws, tax payers must disclose very sensitive and detailed data to authorities in tax returns.² Under national security laws, citizens must not disclose state secrets.³ Beyond such direct legal vectors, various laws drive data disclosures indirectly and in different directions. For example, businesses are enabled and encouraged to restrict disclosures of business secrets under trade secret laws.⁴ Under competition laws, on the other hand, competitors are able to demand access to data.⁵ Whistleblowers are exempt from secrecy obligations to encourage disclosures of information concerning misconduct, wrongdoing and illegal activity.⁶

Privacy and data protection laws contain vectors in different directions concerning data disclosures. One key policy objective of the European Union (EU) General Data Protection Regulation (GDPR) is to remove obstacles to data disclosures within the common market, as evidenced in the title of the ‘regulation [...] on the protection of natural persons with regard to the processing of personal data **and on the free movement of such data**’ (emphasis added).⁷ Also, organizations must disclose data to individual data subjects, data protection officers, and supervisory authorities on request under the GDPR.⁸ But, for the most part, the GDPR points vectors for data disclosures in the other direction, namely against disclosure. Under the GDPR, individuals have rights to prohibit businesses from disclosing or even collecting their personal data⁹ and from transferring personal data across

1 Vector means ‘a quantity that has magnitude and direction’ <www.merriam-webster.com/dictionary/vector> accessed 07.02.2023.

2 Eg German Income Tax Code (EStG) Section 25(3).

3 German Penal Code (StGB) Section 95.

4 Lothar Determann, Luisa Schmaus und Jonathan Tam, ‘Trade Secret Protection Measures and New Harmonized Laws’ (2016) CRI 179 and (2017) Computer & Internet Lawyer 1.

5 Eg <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 07.02.2023.

6 Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] L 157/1, Art. 5(b) and Recital 20.

7 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] L 119/1.

8 Art. 15(4) GDPR.

9 Eg Art. 18 GDPR.

borders.¹⁰ Also, an individual can demand that organizations delete personal data about them.¹¹ More broadly, the GDPR prohibits any processing of personal data, unless individual data subjects consent or other statutory justifications are available,¹² and then only subject to minimization requirements¹³ and extremely broad definitions of what constitutes ‘personal data’, roping in nearly all types of data that humans tend to be interested in.¹⁴ These forceful vectors against data disclosures have increasingly hindered scientific and academic collaboration, information technology development, medical research, precision medicine, public health measures and free exercise of information and communication rights in the EU.¹⁵ As a countermeasure, with vectors encouraging data disclosures, the EU is now debating an EU Data Act ‘for a fair and innovative data economy’¹⁶ instead of modernizing and deregulating its privacy law framework, leaving businesses and individuals in a confusing crossfire of vectors, requirements and prohibitions for and against disclosures.

United States and California privacy lawmakers have traditionally taken a more nuanced approach and mostly focused on ensuring that individual data subjects can make an informed decision about disclosures of personal data, but not outright prohibited or regulated personal data processing.¹⁷ After expressly recognizing a right to privacy in the California Constitution in 1972 pursuant to a popular ballot initiative, California has enacted myriad sector-, harm- and situation-specific privacy law statutes nearly every year.¹⁸ California enacted the first laws worldwide requiring companies to notify individuals of data security breaches (in 2002) and to post website privacy policies (in 2004).¹⁹ More recently, California citizens pushed privacy legislation according to which businesses must specifically

10 Eg Art. 44–49 GDPR.

11 Eg Art. 17 GDPR.

12 Art. 6(1) GDPR.

13 Art. 5(1)(c) GDPR.

14 Art. 4(1) GDPR.

15 Winfried Veil, ‘The GDPR: The Emperor’s New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law’ (2018) NVwZ 686.

16 <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 07.02.2023.

17 Paul M Schwartz, ‘Preemption and Privacy’ (2008) 118 Yale Law Journal 902, 910916; Paul M Schwartz and Karl-Nikolaus Peifer, ‘Transatlantic Data Privacy Law’ (2017) 116 The Georgetown Law Journal 115, 138 et seq.

18 More generally on the adequacy of US privacy laws, see Lothar Determann, ‘Adequacy of data protection in the USA: myths and facts’ (2016) International Data Privacy Law 2016; Lothar Determann, ‘US-Datenschutzrecht – Dichtung und Wahrheit’ [US Data Protection Law – Myths and Facts] (2016) NVWZ 561.

19 Lothar Determann, *California Privacy Law, Practical Guide and Commentary* (4th edn, The Recorder 2020) Ch 1 and Ch 2(N) and (O).

notify Californians about sales of personal information, rights to object to the sale, the right not to be discriminated against in case of opt-out choices, and the value of personal information to the business.²⁰ These novel vectors for data disclosure are far more specifically tailored and suited to protect individual privacy rights than the somewhat outdated concept of a general prohibition with limited exceptions in the GDPR.²¹

This contribution is based on my presentation at said conference and introduces novel vectors for personal data disclosures under California privacy law in Part A, discusses fundamental differences in privacy legislation and data processing regulations in Part B, examines options for lawmakers in Part C, explores policy choices and tradeoffs for lawmakers in other countries in Part D and concludes with a summary and outlook in Part E.

A Data Monetization Trends and Consumer Information Requirements in California

Internet users have to share IP addresses of their devices in order to access websites, location information to see their position on online maps or automatically receive local weather updates, and mobile phone numbers to receive text messages. This is due to technical requirements that Sun Microsystem's CEO famously summed up in 1999 with 'You have zero privacy anyway. Get over it.'²² Internet users may be willing to share additional personal information – which is not strictly required for technical reasons – as consideration for valuable services, in lieu of subscription fees or other payments. For example, companies offer discounts or opportunities to win a prize to consumers who are willing to register for loyalty programs, online accounts, or product trials, or to respond to surveys. Free from the shackles and chains of legacy broadcasting laws, individuals and businesses around the world developed the Internet as a free marketplace for ideas, goods and services.²³ Start-up companies were able to gain critical mass of users for

20 Lothar Determann and Jonathan Tam, 'The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide' (2021) 4 *Journal of Data Protection & Privacy* 7.

21 Art. 6(1) GDPR provides that '[p]rocessing shall be lawful only if and to the extent that at least one of the following applies:' and then lists individual consent and 5 other very limited exceptions that individual persons or organizations must claim to justify any processing of personal data.

22 <www.wired.com/1999/01/sun-on-privacy-get-over-it/>.

23 Lothar Determann, *Kommunikationsfreiheit im Internet* (Nomos 1999).

new innovative services like online maps, social media networks and user-generated content platforms by offering their services free of charge. To fund their operations, businesses sold advertising space and increasingly also personal data of users. Consumers traded data for online services that could never have been established with paid subscription models and mostly felt they received a fair bargain.²⁴

Businesses consider data a valuable asset even if they cannot legally own data.²⁵ In recent years, companies in California and elsewhere have been strategic about collecting personal information for various purposes, including targeting advertisements, generating market insights, improving communications with consumers, developing products, and creating marketable consumer profiles that other companies are willing to pay for.²⁶ As companies have refined their data collection and monetizing methods, consumers have found it increasingly difficult to understand how their data is used, monetized and valued. Consumers and lawmakers have been growing concerned that consumers may be unable to make informed decisions and obtain fair compensation for disclosures of their data. They started questioning the fairness of the data-for-services bargain.²⁷

To empower consumers and strengthen their ability to drive a fair bargain, California lawmakers have insisted on accurate and comprehensible disclosures. In 2004, California enacted the first law worldwide specifically requiring companies to publish website privacy policies.²⁸ Companies are required to inform consumers about their data processing practices under myriad other laws, from Art. 1 of the California Constitution to special rules for Supermarket Club Cards.²⁹ Yet, some consumer and privacy advocates felt that the incremental changes brought by routine advancements of sector-, harm- and situation-specific California privacy laws were not enough.³⁰

In 2018 and 2020, privacy advocates brought about the California Consumer Privacy Act (CCPA) by way of a ballot initiative that also triggered an avalanche of additional legislation and regulations as well as the creation of a California Pri-

24 Lothar Determann, 'Social Media Privacy – 12 Myths and Facts' (2012) *Stanford Technology Law Review* 7.

25 Lothar Determann, 'No One Owns Data' (2018) 70 *Hastings Law Journal* 1.

26 Lothar Determann, 'California data broker registrations: Who made the list on Jan. 31?' (*IAPP Privacy Advisor*, 11 February 2020) <<https://iapp.org/news/a/california-data-broker-registrations-who-made-the-list-on-jan-31/>> accessed 07.02.2023.

27 Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

28 California Online Privacy Protection Act (CalOPPA), California Bus & Prof Code paras 22575–22579.

29 See Determann (n 19) ch 2.

30 See Californians for Privacy <www.caprivacy.org/>.

vacancy Protection Agency, the first agency specifically dedicated to privacy protection in the United States.³¹

Under CCPA, businesses must not discriminate against consumers who exercise their rights to information deletion or object to the selling or sharing of their personal information. At the same time, businesses shall not be prohibited under the CCPA from ‘charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer’s data’ or ‘from offering loyalty, rewards, premium features, discounts, or club card programs.’ The California Attorney General promulgated in 2020 regulations that a business that offers a financial incentive or price or service difference shall provide a ‘notice of financial incentive’ with prescribed disclosures, in addition to ‘at collection notices’, which businesses must generally provide at or before the time they collect personal information from consumers. In the ‘notice of financial incentive’, businesses must disclose material terms of incentive programs, including the value of the consumer’s information.

In enforcement actions concerning failures to provide notices of financial incentive, the California Attorney General offered the businesses 30 days to come into compliance with the CCPA before further enforcement actions would be commenced (as is currently required under the CCPA). In a press release issued by the office of the Attorney General, Bonta ‘urge[d] all business[es] in California to take note and be transparent about how you are using your customer’s data’, signaling an intent to prioritize enforcement of loyalty and other similar consumer programs moving forward.

In notices of financial incentives, businesses must clearly describe the material terms of their financial incentive program. Businesses must include the following information in the notice:

- A succinct summary of the financial incentive or price or service difference offered.
- A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer’s data.
- How the consumer can opt-in to the financial incentive or price or service difference.

³¹ Lothar Determann, ‘Kaliforniens erste Datenschutzbehörde – dank Volksentscheid. California Privacy Rights Act (CPRA) verschärft California Consumer Privacy Act (CCPA) und gilt auch für deutsche Unternehmen’ (2021) ZD 69; Determann and Tam (n 20).

- A statement of the consumer’s right to withdraw from the financial incentive at any time and how the consumer may exercise that right.
- An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer’s data, including:
- A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference.
- A description of the method the business used to calculate the value of the consumer’s data.

A notice of financial incentive must clarify how a consumer can ‘opt in’ (a term not defined in the CCPA), which should not be conflated with a requirement under the CCPA to obtain consent (a defined term in the CCPA). Many financial incentive programs require terms of use and thus a need for an agreement involving some form of consent, anyhow (and in such cases, a separate consent could be added), but there are contexts where companies ask for personal information that may trigger a requirement for a financial incentive notice where terms and conditions may not be required. Per California Civil Code Section 1798.125, a business may enter a consumer into a financial incentive program only if the consumer gives the business prior ‘opt-in consent’ pursuant to Cal. Civ. Code Section 1798.130. But the reference to 1798.130 is confusing because 1798.130 does not provide for how to obtain opt-in consent and, as amended, Section 1798.130 has a heading of ‘notice, disclosure, correction, and deletion requirements’. If the reference is to be given any meaning, it supports that consent is not required before first enrolling a consumer in a financial incentive program because 1798.130(a)(5)(A) requires that businesses include in their CCPA online policy a description of a consumer’s rights pursuant to 1798.125 and methods for submitting requests. There are other possible readings of the CCPA on this point. But the CCPA generally does not require opt-in consent for data collection and has an opt-out structure with regards to selling personal information. It would seem logical that the drafters of the CCPA meant for a similar opt-out regime with respect to financial incentive programs to apply (where opt-in consent and waiting 12 months is only required after someone first opts out). And the title of 1798.125 has been amended to say ‘consumer’s right of no retaliation following opt-out or exercise of other rights’, which would seem supportive of such interpretation.

Businesses now face the difficult task to estimate the value of consumers’ personal information. They should carefully consider all implications from an accounting, tax and litigation perspective. For example, once a business publishes a value pertaining to personal information, the stated value will likely be considered in unrelated contexts and disputes such as data security breaches, trade secret misappropriation, breaches of marketing collaboration contracts with busi-

ness partners, unclaimed property compliance (escheat), or transfer pricing arrangements in multinational groups. Courts will not be bound by the business's valuation, of course, but adversaries may hold a published valuation number against a business as an admission of value and make it difficult to argue for a different valuation.

Consumers may find the additional information helpful to make more informed decisions on how much personal information they want to disclose to a particular business or in the context of a specific service or incentive programs. Also, academics, journalists, privacy advocates, consumer protection association and other information intermediaries will likely conduct studies on value disclosures regarding personal information to help consumers compare offerings and make more informed decisions. At the same time, businesses face skyrocketing costs and challenges in adjusting their privacy law compliance programs to the myriad new and highly prescriptive privacy laws in California and elsewhere.³² Compliance costs are enormous³³ and favor larger and mature organizations, thus raising market entry barriers for start-up companies and reducing competition as well as innovation. With the antidiscrimination provisions in CCPA,³⁴ businesses are vectored to move away from charge-free services models that made the Internet so successful in the first place. Businesses must offer the same level of services to consumers who opt out of personal information selling or exercise other rights under CCPA. It remains to be seen whether consumers will benefit from a fairer bargain, or whether the return to pre-Internet paid subscription business models ultimately drives a reduction in available services, consumer choice, innovation and competition.

B Privacy and Data Protection Legislation

The United States are at a crucial turning point with respect to the protection of individual privacy and regulation of data processing more broadly on a state and federal level. Several states have followed California in enacting comprehensive consumer privacy laws, including Nevada, Virginia, Colorado, Utah and Con-

³² See <www.uschamber.com/major-initiative/data-privacy>.

³³ The California Attorney General's office estimated a \$55 billion cost (approximately 1.8% of California Gross State Product) for initial compliance with the original CCPA, not including costs of ongoing compliance, responses to data subject requests, litigation, and adjusting to the many amendments, see Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (2019) 19.

³⁴ California Civil Code para 1798.125.

necticut by June 2022, with many more bills pending at the state and federal level. Businesses have been pushing for decades for laws at the federal level to preempt the proliferation of diverging US state laws that hamper interstate commerce and innovation.³⁵ Lawmakers and regulators are debating multiple controversial questions, including the following: Should laws governing data processing impose data minimization and prohibitions as a default or continue to focus on individual privacy harms? How should laws reconcile free speech and access to information with the privacy-based ‘right to be left alone’? Should anyone own data? How can governments ensure access to data for law enforcement, national security and governance purposes?

Answers to these questions and corresponding legislative measures are likely to impact the willingness of individuals to disclose personal data and the consideration they expect in return. But, the vectors of personal data disclosures also depend on cultural norms, habits and history, which vary from country to country and state to state within the USA.

I Privacy

Privacy is a sphere that a person controls regarding his mind, thoughts, decisions, communications, body, dignity, home and personal effects, such as papers and smart phones.³⁶ The right to privacy is the right of an individual to be left alone.³⁷ It is a right against other people and legal entities, including family members, neighbors, company representatives and government agents, who may invade a person’s privacy by trespassing, entering a person’s home without permission, accessing personal files on a computer or forcing a person to reveal sensitive personal information about herself.

One can find privacy best where no other people are, in solitude, furthest away from other humans. In civilization, one trades privacy for benefits of living and interacting with others. One lets other people into one’s life to learn, communicate, collaborate, trade, socialize and seek help. One individual’s right to privacy can become an intrusion into another person’s rights to information, free speech or security.

³⁵ See <www.uschamber.com/major-initiative/data-privacy>.

³⁶ Lothar Determann, ‘Privacy Please’ (YouTube, 28 June 2021) <www.youtube.com/watch?v=7u0XNVHXzus>.

³⁷ Samuel D Warren and Louis D Brandeis, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193.

With respect to information specifically, privacy means control over the dissemination of personal information, discretion regarding who may know what about one's body and mind, the choice to remain anonymous, the ability to keep thoughts and communications confidential, and the power to avoid being photographed, filmed or audiotaped.

Individuals feel different needs for data privacy depending on their personal circumstances. A child prodigy living in a large city may physically suffer from excessive invasions into privacy by journalists while a reality television star may welcome any publicity she can get. A dissident may depend on data privacy for his life while an established politician may depend on publicity for his livelihood.

Also, people in different cultures, societies and political systems feel differently about privacy. Americans care deeply about individual freedom, property and privacy in their homes and personal effects, but tend to be less concerned about data collected on public spaces or the Internet.

Germans have created the world's first and strictest regulation of data processing, but they have not coined an exact equivalent of 'privacy' in the German language. In everyday language, Germans may occasionally refer to 'Privatsphäre' (literally translated: 'private sphere') as an abstract sphere and aspect of the general right of personality ('Allgemeines Persönlichkeitsrecht') in which the state and other persons should not interfere. Unlike the US concept of 'privacy', German 'Privatsphäre' is not directly linked to one's home or property. German courts and lawyers additionally use terms like 'informationelle Selbstbestimmung' (information self-determination) and 'Datenschutz' (data protection) with respect to the regulation of data processing, which exists separately from civil law claims pertaining to violations of one's rights to private sphere and personality. The General Data Protection Regulation (GDPR), which is ultimately modelled after German data protection laws, does not mention the term 'privacy' even once.

In Russia, views and terminology regarding privacy have been evolving, particularly since the end of the Soviet Union and communism, which prioritized collective objectives over individual privacy. A direct equivalent of 'privacy' has not yet evolved in the Russian language. 'Приватность' is a modern borrowed term derived from the English term 'private.' 'Конфиденциальность' means literally 'confidentiality' but has been used to translate 'privacy' in the past; for example, 'Privacy Policy' has commonly been translated as 'Политика конфиденциальности.' More recently, 'приватность' is used to translate 'privacy.' The closest equivalent to 'private sphere' is 'Неприкосновенность частной жизни,' which means literally the 'sanctuary of private life' and is used in literature and legislation but not in everyday language. 'Информационная приватность' means 'information privacy' and 'data protection' means 'Защита персональных данных' and is common-

ly found in Russian legislation. For example, the Russian Data Protection Law is called ‘Закон о защите персональных данных’.

In China, the word ‘隐私’ is commonly used to refer to privacy. ‘隐’ means hidden, and ‘私’ means personal, private, and secret. ‘隐私’ commonly refers to private and personal information that an individual prefers to keep secret. One potential difference between the word ‘privacy’ and the word ‘隐私’ is that ‘隐私’ focuses more on the subjective intent of an individual to keep things from other people while ‘privacy’ often refers to the objective state or condition of being free from observation or disturbance by other people. The word ‘隐私’ first appeared in the Zhou Dynasty (1046–256 BCE). Back then, ‘隐私’ meant ‘clothes’; having it or not was thought to be one of the most obvious differences between civilized people and barbarians or beasts.

Around the world, data privacy needs have changed over time and increased exponentially with the development of information technologies. In the 18th century, citizens were most concerned about physical privacy intrusions in the form of arrests, searches and seizures by government agents. In the 19th century, as photography developed, privacy invasion by the press became more noticeable. In the 20th century, computers, data bases and the Internet started to provoke fears of glass citizens, repressive surveillance states and intrusive business practices. Today, mobile phones, connected cars, planes, trains, industrial machines, toys and other devices on the Internet of Things (IoT) generate vast amounts of data and information and the total amount of stored data worldwide is expected to double every two years.

II Privacy Law and Data Processing Regulation

As individuals have felt an increasing need for data privacy over time, states enacted laws protecting privacy. Express references to privacy can be found increasingly in constitutions, international treaties and statutes since the second half of the last century.³⁸

³⁸ David Banisar and Simon Davies, ‘Global Trends in Privacy Protection’ (1999) 8 *Journal of Computer and Information Law* 1 et seq; Lee A Bygrave, ‘Data Protection Pursuant to the Right to Privacy in Human Rights Treaties’ (1999) 6 *International Journal of Law and Information Technology* 247 et seq; Bert-Jaap Koops and others, ‘A Typology of Privacy’ (2017) 38 *University of Pennsylvania Journal of International Law* 483.

1 Constitutional Safeguards

The United States maintain the oldest written constitution. Its bill of rights dates back to 1791 and does not contain an express right to privacy, only a limited prohibition of unreasonable searches and seizures in its fourth amendment. The citizens of the State of California added an express right to privacy to the California Constitution in 1972 by way of a ballot measure in a general election, but there has not been enough consensus in the United States to add such a right to the federal constitution.

Germany enacted its current constitution in 1949 as its ‘basic law’ without expressly referring to ‘privacy’, but protecting human dignity in Art. 1(1), a right to ‘unfold one’s personality’ in Art. 2(1), the confidentiality of mail and telecommunications in Art. 10(1) and the sanctity of one’s home in Art. 13(1). In December 1983, weeks before the turn to the year for which George Orwell had predicted grave intrusions on individual privacy in his novel ‘1984’, the German Constitutional Court recognized an implied right to information self-determination emanating from the express rights to dignity and personality in Art. 1(1) and 2(1) when German citizens challenged an expansive federal census measure.³⁹

Newer constitutions tend to expressly protect a right to privacy, including, for example, the constitutions of Russia (Articles 23, 24 and 25) and South Africa (Section 14).

2 International Treaties

The Universal Declaration of Human Rights of 1948 refers to privacy expressly in Art. 12, as do the subsequently adopted International Covenant on Civil and Political Rights (Art. 17), UN Convention on Migrant Workers (Art. 14), UN Convention of the Rights of the Child (Art. 16), European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8) and the American Convention on Human Rights (Art. 11). The Charter of Fundamental Rights of the European Union does not refer to privacy, but protects a right to ‘private life’ in Art. 7 and the ‘protection of personal data’ in Art. 8.

³⁹ German Constitutional Court, 65 BVerfGE 1 English translation <<https://freiheitsfoo.de/files/2013/10/Census-Act.pdf>> accessed 07.02.2023.

3 Statutes

National statutes protecting privacy have become more common since in 1970 the state Hessen in Germany enacted the first data protection law worldwide. When Governor Oswald signed the Hessian data protection law into force, he referred to George Orwell's novel '1984' and declared that the Hessian data protection law was intended to prevent the surveillance state forecasted by Orwell. Other countries in Europe followed. The European Community then harmonized national data protection laws in Directive 95/46/EC (the 'Data Protection Directive'), which the European Union replaced effective 2018 by a General Data Protection Regulation (GDPR).

More and more countries have followed Europe and also regulated the processing of personal data with general data protection regulations. In August 2018, Brazil enacted a GDPR-like data protection law and India published a GDPR-like bill which has been heavily debated since, but still not been enacted in June 2022.⁴⁰

The United States, on the other hand, had opted against broad omnibus data processing regulation until recently. Since the early 1970s, Congress and state legislatures have been enacting hundreds of sector-, situation- and harm- specific data privacy laws.⁴¹ When California privacy advocates pushed for data processing regulation in the form of CCPA in 2018, the California legislature followed only reluctantly, provoking a second ballot initiative in 2020, which Californians passed with a resounding majority. In other US states, legislatures followed the trend with statutes modelled after CCPA, but this does not change the vector for omnibus data processing regulation in the United States did not originate from parliaments, but rather from privacy advocates and ultimately popular majorities with voters.

III Policy Reasons for Privacy Protections and Limitations

Governments typically protect privacy to safeguard individual human dignity and freedom. Under the shield of data privacy protection, citizens are more empowered to exercise civil rights, such as the freedom of speech, religion and assembly. This in turn helps secure the functioning of the democratic process. Also, citizens need protection from psychological, economic and other privacy harms that states, businesses, criminals and others cause, for example by identity theft; blackmail; bully-

⁴⁰ See Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018' (2018) *Berkeley Journal of International Law*.

⁴¹ Schwartz (n 17).

ing; stalking; revelation of secret location or identities of spies, domestic abuse victims or persons in witness protection programs; stigmatization based on addictions, diseases, political opinions, religion, race or sexual preferences; computer hacking; irritating direct marketing methods; unfair business practices based on surreptitious data collection; and discrimination by employers, banks and insurance companies based on information about pre-existing health conditions.⁴²

There are also reasons why – and situations when – governments do not protect, but rather invade privacy. The executive branch of governments fulfils many functions, most importantly law enforcement, that necessitate data processing and tend to collide with privacy protection agendas. Additionally, legislatures and courts also safeguard interests and policy objectives that conflict with data privacy, such as freedom of information and commercial enterprise. One person's right to gather and share information on another person can intrude on the other person's interest in data privacy. Different jurisdictions balance these conflicting policy goals differently.

The U.S., for example, tends to hold freedom of speech, information and commercial enterprise in relatively high regard and therefore decided against enacting the kind of omnibus data protection laws that are prevalent in Europe. Also, after the terrorist attacks of September 11, 2001, the United States has been very focused on national security and ramping up government surveillance programs. In Europe, on the other hand, people still remember what surveillance by totalitarian regimes has done to them. European lawmakers have decisively acted to limit the automated processing of personal data and carved out narrowly defined exceptions for press, media and non-commercial activities. Anyone trying to understand, interpret and apply data privacy laws has to consider the various conflicting interests and their relative status in the applicable legal system.

Without security, there can be no privacy; criminals, companies and foreign governments will invade individual privacy if security is not safeguarded. There can be security without any privacy, though. A totalitarian state focused on absolute security will monitor all individuals at the expense of their privacy. But, this is not necessary and reasonable degrees of security and privacy can co-exist. There

⁴² Danielle K Citron, 'Sexual Privacy' (2019) *Yale Law Review*; Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087; Daniel J Solove and Danielle K Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2018) *Texas Law Review*; Ryan Calo, 'Privacy Harm Exceptionalism' 12 *Colorado Tech Law Journal* 361 (2018); Amit Datta and others, 'Automated Experiments on Ad Privacy Settings' (2015) *De Gruyter Open*; Margaret Hu, 'Big Data Blacklisting' (2015) 67 *Florida Law Review* 1735, 1809; Mikella Hurley and Julius Adebayo, 'Credit scoring in the era of big data' (2016) 18 *Yale Journal of Law & Tech* 148, 151; Danielle K Citron and Frank Pasquale, 'The Scored Society: Due Process For Automated Predictions' 89 (2014) *Washington Law Review* 15.

cannot be free speech and democracy without privacy or security. Societies have to strike a balance with respect to privacy and security.

C Legislative Approaches

The terms ‘data privacy’ and ‘data protection’ are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Also, data security, data residency, data retention, data ownership and trade secret requirements are often thrown into the mix. But, the approaches, purposes and effects are quite different.

I Privacy Protection

The individual person and her autonomy is the central focus of privacy laws. Data privacy laws are intended to protect individuals from intrusion into reasonable privacy expectations, interception of confidential communications and other specific privacy harms.

Data privacy laws typically contain requirements regarding notice, choice, data security and sanctions. Individuals must be notified about how their data is handled so they can decide how much information they share, with whom and for what consideration. If they have access to sufficient information in privacy policies and other notices, they can adjust their conduct or privacy expectations. In particularly sensitive scenarios, companies may need to obtain express and informed consent. If companies fail to live up to their commitments in privacy policies or apply reasonable security safeguards and cause harm, then individuals can assert claims in private lawsuits including class actions. Regulators and law enforcement authorities can also sanction offenders in particularly egregious privacy law violations.

II Data Protection

The processing of personal data is the central focus of data protection laws. European legislatures have taken George Orwell’s warnings to heart and view automated data processing as an inherently dangerous activity warranting strict regulation.

The GDPR, like previous EU data protection regulation, builds restrictions and limited exceptions around a fundamental prohibition of any processing of personal

data in Art. 6(1) GDPR. European data protection laws are first and foremost intended to restrict and reduce automated processing of personal data. Individual privacy expectations, harm potential, choice or consent are not predominantly relevant. Accordingly, broad definitions of ‘personal data’ and ‘processing’ prevail and even publicly available data is covered. Companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods for which they retain data.

Besides basic prohibitions and minimization principles, data protection regulations typically establish data protection authorities, impose registration and approval requirements, prescribe filing fees, mandate the designation of local representatives and internal data protection officers, restrict international data transfers, mandate data protection impact assessments and require that companies maintain data inventories and accountability documentation that data protection authorities can routinely audit. Data protection authorities are also primarily tasked with enforcing data protection laws.

Data protection laws can indirectly benefit individual privacy if they cause companies and governments to process less personal data. But, protecting individual privacy is not the direct focus of the GDPR or other EU data protection laws. Individual privacy expectations, needs or harms can factor into data protection impact assessments, determinations whether security breaches have to be notified under Art. 33 or 34 GDPR, and the application of Art. 6(1)(f) GDPR, the ‘legitimate interest exception’ to the general prohibition of automated data processing. But, many other requirements and restrictions apply regardless of individual privacy considerations.⁴³

III Information Access Blocking Prohibitions

Overly restrictive vectors against data disclosures create needs for corrections. In the EU, data processing regulation has literally become unhealthy.⁴⁴ But instead of modernizing and deregulating data processing regulations, EU lawmakers are debating corrections in the form of an EU Data Act ‘for a fair and innovative data economy’.⁴⁵ At the same time, competition law authorities pressure companies

⁴³ For a review of the GDPR as ‘the law of everything’, see Helen Dixon and Lothar Determann, ‘International Privacy Law – Year in Review’ (*Baker McKenzie*; 10 May 2022) <<https://www.bakermckenzie.com/en/insight/publications/2022/06/international-privacy-year-in-review-for-us-practitioners>> accessed 07.02.2023.

⁴⁴ Lothar Determann, ‘Healthy Data Protection’ (2020) 26 *Michigan Tech Law Review* 229.

⁴⁵ <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 07.02.2023.

to provide access to data to competitors and refrain from implementing compliance measures that EU data processing regulations and electronic communications privacy laws seemingly require.⁴⁶

In the United States, counter-measures to data processing regulations have largely been unnecessary, because lawmakers had narrowly tailored privacy laws to protect individual rights in sector-, harm- und situation-specific laws. But, the ‘information blocking’ prohibitions in the US Cures Act are a sector-specific example of countermeasures to redirect unhealthy vectors against medical data disclosures resulting from US federal health privacy laws.⁴⁷ Originally, US lawmakers sought to promote responsible medical data disclosures for treatment, research and patient access purposes in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), subject to safeguards in Privacy and Security Rules.⁴⁸ Apparently, some healthcare providers and other covered entities continued to release health information only sparingly, even where HIPAA mandated or allowed medical data disclosures, possibly due to the overwhelming complexity of HIPAA and its associated rules.⁴⁹

More generally, companies are vectored in confusingly different directions based on privacy, competition and consumer protection policy mandates in the United States. While the FTC punishes one social media network for enabling other companies to access its publicly available data too easily with a \$5bn fine, the 9th Cir Court of Appeals prohibits another social media network from applying restrictions to data access designed to protect user privacy.⁵⁰ Businesses and individuals are caught in a confusing crossfire of vectors, requirements and prohibitions for and against disclosures.

⁴⁶ Eg <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 07.02.2023; <<https://digiday.com/media/why-googles-approach-to-replacing-the-cookie-is-drawing-antitrust-scrutiny/>> accessed 07.02.2023.

⁴⁷ Eg <www.healthit.gov/topic/information-blocking> accessed 07.02.2023.

⁴⁸ Mark A Rothstein, ‘HIPAA Privacy Rule 2.0’ (2013) *Journal of Law, Medicine and Ethics* 525.

⁴⁹ See Craig Konnoth, ‘Regulatory De-Arbitrage in Twenty-First Century Cures Act’s Health Information Regulation’ (2020) *Annals of Health Law*.

⁵⁰ See <<https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>> accessed 07.02.2023 and *HiQ v. LinkedIn* [2022] USCOA No 17–16783.

IV Data Security Laws

Legislatures around the world have started to supplement data privacy laws with increasingly specific data security laws that aim to protect individuals from specific harms resulting from unauthorized access to personal information, in particular identity theft. Examples include data security breach notification laws: California passed the first law in 2002, with most US states and many countries following suit thereafter. Also, more and more laws prescribe encryption or other technical and organizational measures, also known as ‘TOMs’. In 2018, California added a duty on manufacturers of connected devices to design products with reasonable security measures and refrain from delivering products with default passwords, for example. Data security measures limit unauthorized access to information and thus protect data and individual privacy.

V Trade Secret Laws

Businesses use contracts and tort laws to protect confidential information from misappropriation by unauthorized persons. As a condition to trade secret claims, companies have to prove that they used reasonable efforts to keep their information secret, which often includes similar measures as required by data security laws with respect to personal data. Where confidential business information pertains to persons (as opposed to technologies or manufacturing processes, for example), trade secret law can also indirectly protect individual privacy. But, the primary purpose of trade secret laws is to protect business integrity and competition from unfair misappropriation of valuable confidential information.

VI Data Ownership

With property laws, states allocate real estate, chattels, intangibles or other items to individuals with an entitlement to exclude others in the interest of incentivizing innovation, creation, maintenance and investment regarding the allocated items. Legislatures typically exclude information as such from the scope of property laws, to preserve maximum public access. Also, it seems hardly necessary or in the public interest to incentivize the creation of information. Even without rewards in the form of property rights, companies and governments hoard enough data at the expense of individual privacy.

If individuals owned personal data about themselves, they could theoretically gain additional rights to defend their privacy. In practice, however, many individ-

uals would likely be induced or compelled to sell their personal data property rights, with the undesirable effect that the buyers could exclude the data subjects from personal information about themselves. Others could use property rights to withhold information about themselves that governments, companies or individuals legitimately need for public safety, security or other purposes. Therefore, no one owns or should own data.⁵¹

VII Freedom of Speech and Information

Individuals and their right to communicate and inform themselves is the core function of constitutional freedoms of communication and information. Privacy rights can directly conflict with rights to free speech and information. For example, defamation claims, censorship measures and ‘rights to be forgotten’ can be based on privacy laws and restrict the dissemination of information or access to data. Privacy rights can also complement rights to free speech and information, because people can speak more freely when they can remain anonymous or at least hide or obscure their identities from government or private prosecution. But, freedoms of speech and information do not typically protect privacy and rather intrude.

VIII Data Residency and Retention Requirements

Governments mandate that companies and citizens maintain certain documentation, records and information locally for minimum time periods, to be available for tax audits, law enforcement investigations and national security monitoring. Russia, Kazakhstan, Indonesia and the People’s Republic of China have enacted particularly broad data residency requirements that are not limited to particular types of records but all personal data.⁵² Data residency and retention laws are not intended to protect privacy. To the contrary, such laws limit individual privacy. European Union laws requiring companies to store Internet meta data for minimum time periods have been successfully challenged and invalidated based on constitutional safeguards for data privacy.⁵³

⁵¹ Determann (n 25).

⁵² Lothar Determann, ‘Data Residency Rules Cutting Into Clouds: Impact and Options for Global Businesses and IT Architectures’ (2017) Bloomberg BNA Data Privacy & Security Law Report.

⁵³ German Constitutional Court 1 BvR 256/08, (2010) NJW 833; Case C-293/12 Digital Rights Ireland v Ireland [2014] European Court of Justice 62012CJ0293.

D International Privacy Law at Crossroads

More and more countries are enacting or updating privacy laws based on one or more of the approaches described in the preceding Part C of this contribution. Many jurisdictions enact European-style data processing legislation and few follow the United States.⁵⁴ In fact, the United States itself is currently reconsidering its own approach. International privacy laws are at crossroads.

I Privacy v. Data Protection

When Hessen and then other German states and European countries started enacting data protection laws in the 1970s, the United States also considered this option, but decided against comprehensive regulation of data processing. Congress felt it was too early to appropriately identify and address potential privacy harms and balance privacy interests with freedom of information, innovation and economic freedoms.⁵⁵ Therefore, the United States resolved to pass sector-, situation- and harm-specific privacy laws as the need arises, at the state and federal level. This allowed information technology companies in the Silicon Valley to grow and become industry leaders in semiconductor technologies, software, e-commerce, cloud computing, social media, big data and other data intensive products and services.⁵⁶ But, this also resulted in hundreds of diverging and constantly evolving privacy laws across the United States. Companies and government agencies find it increasingly difficult to navigate the maze of US privacy laws. Businesses are particularly concerned about the California Consumer Privacy Act of 2018, which adds extensive new disclosure requirements and individual rights to existing laws in order to reign in perceived risks emanating from data selling.⁵⁷

Calls have become louder for uniform federal privacy laws in the United States. Politicians, government authorities, activists, businesses and consumers agree in principle that broad federal legislation is warranted. Disagreements prevail, however, over important questions of detail, including whether a new federal law should preempt (that is: invalidate) or merely supplement existing state laws, and whether the United States should adopt European-style data processing regulations or continue the US tradition of individual privacy protections.

⁵⁴ See for a recent overview Dixon and Determann (n 43).

⁵⁵ Schwartz (n 17).

⁵⁶ Anupam Chander, 'How Law Made Silicon Valley' (2014) 63 *Emory Law Journal* 639.

⁵⁷ Determann (n 19) Ch 2–26a.

II Adequacy of EU Regulations of Data Processing

The EU hails its GDPR as the most modern data protection law worldwide and claims authority in Art. 45 GDPR to formally decide whether the level of data protection in other countries is adequate. At the same time, critics, including in the German government, are questioning whether the GDPR itself is truly adequate.⁵⁸ The European approach from the 1970s to broadly prohibit processing of personal data, subject to a limited number of exceptions, seems even more unrealistic and impractical today where information technologies are so developed and omnipresent. European calls to elevate privacy to a fundamental human right may be merely ‘rights talk.’⁵⁹

When some refer to the GDPR as the ‘gold standard for privacy laws,’⁶⁰ it seems worth asking whether a gold standard is desirable in 2022 and preferable over modern monetary policy and crypto currencies. Granted, some may be happier with owning gold than with owning bitcoin in June 2022, after spectacular devaluations in recent days. Also, some may prefer to live in a world without computers and automated processing of personal data. Yet, the GDPR seems hardly more modern or progressive than the gold standard in the currency sphere. Both seem outdated and ill-suited to safeguard competing policy interests in modern economies and information societies.

The genie is out of the bottle. Data processing technologies are here to stay. Data collection, usage and sharing will increase, in fact: must increase, to better research and cure diseases; treat patients with personalized, precision medicine; develop artificial intelligence; enable autonomous cars to recognize and protect people; support global communications; create reliable block-chains; and protect national and international security. EU-style data minimization and prohibitive regulation is counter-productive to pursuing the many opportunities of data-driven innovation. Also, vast amounts of sensitive personal data on most people is already stored in numerous legitimate and illegal data bases around the world.⁶¹

European companies and governments are using – and will continue to use – very similar technologies, products and services as their US counterparts. Today, most information technologies, products and services are developed by industry leaders outside of Europe, but individual data subjects in Europe are exposed to

⁵⁸ Veil (n 15).

⁵⁹ Schwartz (n 17); Schwartz and Peifer (n 17).

⁶⁰ Alessandro Mantelero, ‘The Future of Data Protection: Gold Standard vs. Global Standard’ (2020) Computer Law & Security Review.

⁶¹ Robert McMillan, ‘Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks’ *WSJ* (Washington DC, 10 December 2018).

the same privacy harms and concerns in the EU as elsewhere. Also, omnibus data protection laws that try to regulate everything⁶² are unreasonably vague and difficult to update. It took the European Union more than 20 years to replace the Data Protection Directive with the GDPR effective 2018. Moreover, the Data Protection Directive of 1995 merely constituted a harmonized version of national data protection laws from the 1970s, before private television, the Internet, mobile phones, big data, cloud computing and other technologies arrived on the scene.

III Why Then Follow Europe?

Despite the obvious shortcomings of European data protection laws, more and more countries outside Europe have enacted similar laws. One reason are benefits for cross-border trade if the EU finds data protection laws of another country ‘adequate’. The procedure contemplated by the Data Protection Directive and also in the GDPR has yielded somewhat surprising results: Since 1995, only Argentina, Canada, Israel, Japan, Korea, New Zealand, Uruguay and a few smaller countries have been found to have ‘adequate levels of data protection’. Another reason is that the United States approach has become unmanageable in practice. In the 1970s, the United States shied away from enacting European-style general data protection laws for fear such laws could suffocate innovation and become too difficult to update and supplement as privacy threats evolve. Since then, the United States enacted and updated hundreds of threat- or sector-specific privacy laws, each narrowly crafted, but cumulatively suffocating in their own way. The California Consumer Privacy Act of 2018 (CCPA) imposes overly complex and detailed obligations on companies that are not compatible with requirements of other jurisdictions. Businesses can no longer navigate the maze. The United States need a reform centered around federal legislation.

But, perhaps the most important reason is that crafting tailored and balanced privacy laws is very difficult. Lawmakers find it relatively easy to craft data security and data protection legislation. Anyone can agree on what good *security* looks like: unauthorized persons do not have access to confidential information. Also, if one accepts with EU lawmakers that the processing of personal data is predominantly harmful and dangerous, then one can easily agree on data minimization and the various procedural and administrative requirements contained in the GDPR.

62 For a review of the GDPR as “the law of everything”, see Dixon and Determann (n 44).

Crafting balanced and proportionate privacy laws focused on preventing harm while protecting free speech, information and innovation, however, is much more difficult. We do not all agree on what good *privacy* looks like. A defendant who demands that the police stay out of his home or computer obstructs criminal investigations or national security measures. A patient who objects to clinical trials or research prevents medical progress and cures. An employee who objects to workplace monitoring makes it harder for employers to prevent harassment and theft of trade secrets. A politician who demands a ‘right to be forgotten’ intrudes on freedoms of speech and information rights of other citizens.

Data subjects are not harmed by the processing of personal data as such. Concerns pertain to particular abuses of data processing, such as discrimination by employers, health insurance companies and law enforcement. But, it is difficult for policymakers to agree on the dividing lines between legitimate use and abuses. For example, some believe that insurance companies should be permitted to consider how healthy policy holders (people) live and offer discounts to non-smokers or based on exercise and eating habits to encourage lower risk behaviors. Others see an unfair penalty for smokers or overweight people and feel violated in their privacy if insurance companies monitor their exercise levels and consumption habits.

Moreover, it is difficult to enforce laws that are narrowly focused on prohibiting certain abuses. It is much easier to just prohibit the collection of personal data in the first place, so the data cannot be abused. But, this seems like an overkill. States do not prohibit cars to reduce car accidents either and instead enact differentiated traffic rules, even if they are harder to craft and enforce than a complete prohibition of cars. Similarly, we need differentiated rules focused on privacy harms, which need to be constantly updated as technologies and threats evolve.

Policymakers should focus on particular privacy harms and craft legislation that balances privacy and other interests proportionally. Legislatures should not continue with the European approach of broadly prohibiting or regulating the processing of personal data, because this has not led to effective privacy protections in Europe in the past and only prevented scientific and commercial progress in the information technology sector, which is now globally dominated by non-European companies. Data processing as such is not harmful to individuals, but necessary and largely beneficial. Lawmakers should encourage and enable secure data sharing and direct their efforts to enforce existing laws to prevent and pursue abuses such as cybercrime, fraud and harmful discrimination. If lawmakers enact broadly applicable general privacy laws to define baselines, they must be careful to prevent ossification and leave room for updates and upgrades as technologies and business practices evolve and new threats emerge.

E Conclusion and Outlook

The United States and other countries find themselves at crossroads with respect to data-related policies. The rigid regulatory and prohibitive approach in Europe has hindered the development of information technologies in Europe. The GDPR repeats and doubles down on regulatory concepts of the 1970s by broadly restricting data collection, retention, transfers and other processing. In the 2020s, this blunt vector hardly promises adequate answers for today's or tomorrow's data-related challenges. Countering harmful effects of restricting data sharing with an even more complex regime requiring data sharing under the EU Data Act proposal threatens further confusion and misdirection through inconsistent and incomprehensive vectoring.

Technology companies have fared better in the United States under narrowly crafted privacy laws, but evolving technologies and privacy threats have triggered so many specific laws that the legal environment has become unmanageably complex. Data privacy law reform should focus on actual harms and remain flexible to allow frequent updates and adjustments as technologies and threats evolve. Yet, California voters have decided in the 2020 general election by way of popular ballot measure to abandon the United States' historic approach of sector-, harm- and situation-specific privacy laws in favor of omnibus data processing regulation adopting elements found in the GDPR. The people have spoken.

Aside from being overbroad and overly complex, however, California privacy laws also contain novel and interestingly nuanced vectors: By requiring businesses to inform consumers specifically regarding the value of personal information in 'notices of financial incentives', providing detailed disclosures regarding information processing practices, and offering opt-out rights concerning selling and sharing of personal information, California has fortified existing consumer rights. Consequently, consumers may become able to better understand and exercise their rights and bargaining powers concerning personal information in online and off-line market places. This should allow lawmakers to peel back other laws and regulations to positively and consistently shape policy-focused vectors for personal data disclosures in California and elsewhere.

More broadly, lawmakers should address data policy holistically within coherent and understandable legislative frameworks instead of unleashing confusingly complex and disparate vectors concerning data disclosures on businesses and individuals – as in the GDPR and the EU Data Act in Europe or in the United States in the HIPAA Privacy Rule and information blocking prohibitions in the U.S. Cures Act. Precisely aimed, modern vectors for thoughtful data disclosures as in the CCPA can be effective only if businesses and consumers are enabled to understand

and follow them. Lawmakers have to repeal, simplify and realign the thicket of existing data-related legislation in Europe and in the United States.



DATA PRIVACY

United States: California Attorney General sets sights on consumer loyalty programs for CCPA enforcement

BY LOTHAR DETERMANN, HELENA J. ENGFELDT AND TERESA MICHAUD - APRIL 7, 2022 - 6 MINS READ

In brief

On "Privacy Day" – California Attorney General Rob Bonta announced an **investigative sweep** targeted at the data collection practices of businesses running consumer loyalty programs in California and issued notices of non-compliance to a number of "major corporations" in the retail, home improvement, travel, and food services industries. Such loyalty programs offered financial incentives to consumers (e.g., discounts, free items, and other rewards) in exchange for their personal information.

Under the California Consumer Privacy Act of 2018, as amended by the Consumer Privacy Rights Act of 2020 (CCPA), businesses must not discriminate against consumers who exercise their rights to information deletion or object to the selling or sharing of their personal information. At the same time, businesses shall not be prohibited under the CCPA from "charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data" or "from offering loyalty, rewards, premium features, discounts, or club card programs".

The California Attorney General promulgated in 2020 regulations that a business that offers a financial incentive or price or service difference shall provide a "notice of financial incentive" with prescribed disclosures, in addition to "at collection notices", which businesses must generally provide at or before the time they collect personal information from consumers. In the "notice of financial incentive", businesses must

disclose material terms of incentive programs, including the value of the consumer's information.

In the recent enforcement actions concerning failures to provide notices of financial incentive, the California Attorney General offered the businesses 30 days to come into compliance with the CCPA before further enforcement actions would be commenced (as is currently required under the CCPA). In a press release issued by the office of the Attorney General, Bonta "urge[d] all business[es] in California to take note and be transparent about how you are using your customer's data", signaling an intent to prioritize enforcement of loyalty and other similar consumer programs moving forward.

The notice of financial incentive must clearly describe the material terms of the financial incentive program, be readily available before a consumer opts in, and inform consumers that they may opt-out at any time. Specifically, a business must include the following in the notice:

1. A succinct summary of the financial incentive or price or service difference offered.
2. A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data.
3. How the consumer can opt-in to the financial incentive or price or service difference.
4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right.
5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:
 - A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference.
 - A description of the method the business used to calculate the value of the consumer's data.

It is clear that the notice of financial incentive must include how a consumer can "opt-in" (a term not defined in the CCPA), which should not be conflated with a requirement under the CCPA to obtain consent (a defined term in the CCPA). Many financial incentive programs require terms of use and thus a need for an agreement involving some form of consent, anyhow (and in such cases, a separate consent could be added), but there are contexts where companies ask for personal information that may trigger a requirement for a financial incentive notice where terms and conditions may not be required. Per Cal. Civ. Code Section 1798.125, a business may enter a consumer into a financial incentive program only if the consumer gives the business prior "opt-in

consent” pursuant to Cal Civ. Code Section 1798.130. But the reference to 1798.130 is confusing because 1798.130 does not provide for how to obtain opt-in consent and, as amended, section 1798.130 has a heading of “notice, disclosure, correction, and deletion requirements”. If the reference is to be given any meaning, it supports that consent is not required before first enrolling a consumer in a financial incentive program because 1798.130(a)(5)(A) requires that businesses include in their CCPA online policy a description of a consumer’s rights pursuant to 1798.125 and methods for submitting requests. There are other possible readings of the CCPA on this point. But the CCPA generally does not require opt-in consent for data collection and has an opt-out structure with regards to selling personal information. It would seem logical that the drafters of the CCPA meant for a similar opt-out regime with respect to financial incentive programs to apply (where opt-in consent and waiting 12 months is only required after someone first opts out). And the title of 1798.125 has been amended to say “consumer’s right of no retaliation following opt-out or exercise of other rights”, which would seem supportive of such interpretation.

Businesses now face the difficult task to estimate the value of consumers’ personal information. They should carefully consider all implications from an accounting, tax and litigation perspective. For example, once a business publishes a value pertaining to personal information, the stated value will likely be considered in unrelated contexts and disputes such as data security breaches, trade secret misappropriation, breaches of marketing collaboration contracts with business partners, unclaimed property compliance (escheat), or transfer pricing arrangements in multinational groups. Courts will not be bound by the business’s valuation, of course, but adversaries may hold a published valuation number against a business as an admission of value and make it difficult to argue for a different valuation.

Our team is monitoring developments as the cure period for compliance provided in the notice nears expiration. Should you have questions in the meantime, please reach out to our team or your Baker McKenzie contacts for additional information.

CATEGORIES:

DATA PRIVACY

NORTH AMERICA

PRODUCT REGULATION & LIABILITY

USA

**Lothar Determann**

Lothar Determann has been helping companies in Silicon Valley and around the world take products, business models, intellectual property and contracts global for nearly 20 years. He advises on data privacy law compliance, information technology commercialization, interactive entertainment, media, copyrights, open source licensing, electronic commerce, technology transactions, sourcing and international distribution at Baker McKenzie in San Francisco & Palo

Alto. He is a member of the Firm's International/Commercial Practice Group and the TMT and Healthcare industry groups.



Helena J. Engfeldt

Helena Engfeldt helps companies around the world expand their businesses internationally especially by taking contracts, intellectual property, and privacy law compliance global. She is a partner in Baker McKenzie's International/Commercial Practice Group in San Francisco. She is licensed to practice law in California and New York.



Teresa Michaud

Teresa H. Michaud advises on all aspects of dispute resolution, primarily complex business disputes, class actions, intellectual property and international arbitration. She is the Co-Chair of the North American Class Action Subgroup and practices in both the Consumer Goods & Retail and Technology, Media & Telecom Global Industry Groups. She is admitted to practice in California, Texas and New York, and qualified in England and Wales. She is a Certified Information Privacy Professional/United States (CIPP/US). Teresa is also one of the founding members of our Los Angeles office that opened in 2018.

Related Posts

European Commission updates "Guidance on non-preferential rules of origin"

APRIL 14, 2022

United Kingdom: UK's Plastic Packaging Tax enters into force

APRIL 14, 2022

United States: SEC Issues Long-Awaited Climate Disclosure Rule Proposal

APRIL 13, 2022

Write A Comment

Enter your comment here..

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT



Archives

Select Month▼

© Copyright 2022 – Global Compliance News

[Disclaimers](#) | [Privacy Statement](#) | [Attorney Advertising](#)

The Employer Report


NAVIGATING US AND GLOBAL EMPLOYMENT LAW

California Becomes First State to Require Venture Capital Companies to Report Diversity Data From Portfolio Company Founders



[Maarten van den Heuvel](#), Unsplash



 Listen to this post

In first-of-its-kind legislation, under [SB 54](#), California will require venture capital companies to collect and report diversity data from portfolio company founders as soon as **March 1, 2025**. The new *Fair Investment Practices by Investment Advisers* law intends to increase transparency regarding the diversity of founding teams receiving venture funds from covered entities in California.

Covered Entities

Venture capital companies are covered by the new requirements if they:

1. Primarily engage in the business of investing in, or providing financing to, startup, early-stage, or emerging growth companies, or manage assets on behalf of third-party investors, including, but not limited to, investments made on behalf of a state or local retirement or pension system; and
2. Have a nexus to California, by:
 - Being headquartered in California;
 - Having a significant presence or operational office in California;
 - Making venture capital investments in businesses that are located in, or have significant operations in, California; or
 - Soliciting or receiving investments from a person who is a resident of California.

Key Reporting Requirements

Starting March 1, 2025, and annually thereafter, covered entities must report specified information about the founding teams of all businesses in which the covered entity made a VC investment in the prior calendar year and certain other investment information to the California Civil Rights Department. (CRD is the government agency that collects pay and demographic data from private employers of 100 or more employees in California.)

- **Founder Demographic Data**

Covered entities must report, at an aggregated level, for each member of the founding team (to the extent information was provided, as disclosing information by founding team members is voluntary and they will not be penalized for declining to answer), such person's gender identity, race,

ethnicity, disability status, sexual orientation, veteran status, and whether such person has California residency. Data must be provided to CRD on an aggregated level and anonymized basis.

- **Investment in Diverse Funding Teams Data**

Covered entities must also report the total number and dollar amount (each, as a percentage of total VC investments made) of VC investments to businesses primarily founded by diverse founding team members, aggregated and broken down by each of the above categories.

“Primarily founded by diverse founding team members” means more than half of the founding team members responded to the annual survey, and at least half of the founding team members self-identify as a woman, nonbinary, Black, African American, Hispanic, Latino-Latina, Asian, Pacific Islander, Native American, Native Hawaiian, Alaskan Native, disabled, veteran or disabled veteran, lesbian, gay, bisexual, transgender, or queer.

Further, covered entities must disclose the total amount of money in VC investments the covered entity invested in each business during the prior calendar year and the principal place of business of each company in which the covered entity made a VC investment during the prior calendar year.

Privacy Notice

VC companies that are subject to the California Consumer Privacy Act (CCPA) are required to provide a privacy notice at or before the point of collection of personal information to California resident founders and account for the new data processing in its online CCPA privacy policy.

Information on racial or ethnic origin and sexual orientation are categories of “sensitive personal information” that receive additional protections under the CCPA. Businesses are allowed under the CCPA to use sensitive personal information as necessary to comply with applicable law (such as this one). And VC companies remain free to use sensitive personal information without inferring characteristics, which should cover most legitimate use cases to satisfy the reporting requirement. VC companies that do infer characteristics based on racial or ethnic origin or sexual orientation information of a California resident would have to carefully analyze restrictions, compliance requirements, and risks under existing civil rights and anti-discrimination laws.

Failing to Report

Failure to timely file a report will prompt the CRD to notify the covered entity that it must submit a report within 60 days of the notification. Further failure may result in an enforcement action by the CRD.

The legislation empowers the CRD to seek court orders to compel compliance, impose penalties to deter future non-compliance, recover its attorney's fees, and grant other relief as deemed appropriate.

What's Next

SB 54 was adopted in the context of increased scrutiny of ID&E efforts.

Earlier this year, the U.S. Supreme Court banned the use of race-conscious admission policies in higher education (see our prior article [HERE](#)), and last year, a California court found that a prior bill, AB 979, requiring publicly held corporations with a principal executive office in California to include at least one director from an underrepresented community (including individuals who self-identify as Black, African American, Hispanic, Latino, Asian, Pacific Islander, Native American, Native Hawaiian, or Alaska Native, or who self-identify as gay, lesbian, bisexual, or transgender) was unconstitutional (see our prior article [HERE](#)).

On October 18, 2023, the Court of Appeals for the Fifth Circuit decided against plaintiffs who challenged a Nasdaq stock market rule that requires listed companies to disclose board diversity data, *Alliance for Fair Board Recruitment et al. v. SEC*, case number 21-60626. Plaintiffs asserted that the Nasdaq rule would cause unconstitutional discrimination, but the court ruled that the SEC only accepted and did not propose the rule and that Nasdaq is a private entity not subject to constitutional scrutiny.

SB 54 may become subject to similar legal challenges that may delay implementation. However, the VC companies should assess their internal capabilities to prepare for collecting the required information for investments made during calendar year 2024 in order to comply with the reporting obligations and meet the expected March 1, 2025 reporting deadline.

**Baker
McKenzie.**

The Employer Report

**Baker
McKenzie.**

California's CCPA forums are underway: Here's what happened at the first one

🕒 Jan 11, 2019

📌 Save This ()



Lothar Determann Lothar Determann

The California Attorney General is holding [six statewide forums](https://oag.ca.gov/news/press-releases/attorney-general-becerra-hold-public-forums-california-consumer-privacy-act-part?mkt_tok=eyJpIjoiTTJGaE5UVmlNaV3WVRFcSIsInQiOiJUNE50QmoydFwvSOY3QkRMZDArS3VlRm1aV3RCeFlZbDI5c3lXd3BhUDBlbHZEcXA4ZzRwK09HVVdnZ) (https://oag.ca.gov/news/press-releases/attorney-general-becerra-hold-public-forums-california-consumer-privacy-act-part?mkt_tok=eyJpIjoiTTJGaE5UVmlNaV3WVRFcSIsInQiOiJUNE50QmoydFwvSOY3QkRMZDArS3VlRm1aV3RCeFlZbDI5c3lXd3BhUDBlbHZEcXA4ZzRwK09HVVdnZ) to collect feedback on the California Consumer Privacy Act to "solicit broad public participation." On Jan. 8, I attended the first hearing on a rainy day — finally! — here in San Francisco. Here are some of my observations.

Attorneys, law professors, data security professionals, data scientists, students, reporters and representatives of various organizations filed into the Milton Marks Conference Center near City Hall before 10 a.m., while representatives of the California Department of Justice explained the purpose of the hearings and asked for comments on the rule-making topics contemplated by the CCPA.

Topics include adding categories of personal information and updating the definition of unique identifiers to address changes in technology and privacy concerns; establishing exceptions necessary to comply with state or federal law, including those relating to trade secrets and intellectual property rights; and establishing rules, procedures and exceptions to ensure that notices and information are provided in a manner that may be easily understood by the average consumer

Each audience member had the floor and microphone for up to five minutes of public comments, which included requests for clarifications, flags of technical errors, suggestions for reductions in scope, pleas to expand privacy protections further, and general criticisms of the CCPA.

Commentators at the hearing acknowledged the difficulties that the attorney general faces since the rule-making pertains to a statute that is still subject to ongoing legislative change and correction of obvious typos and drafting errors. Some asked for a clarification that the term "consumer" does not extend to employees. Others noted that the CCPA's de-identification standard is nearly impossible to meet except by way of aggregation. One attendee suggested that the attorney general publish template privacy notice formats and offer a safe harbor to companies that voluntarily adopt the templates, as the California Civil Code already offers for breach notices, without mandating the use of templates.

Hearing participants also proposed ramped-up time periods for companies that become subject to the CCPA during a calendar year due to increasing revenue; clarifications that companies should not be required to collect or combine personal information to identify consumers for purposes of responding to information access or deletion requests if the companies had not previously identified such consumers; and an ability for businesses to charge for information access and deletion requests or opt-out declarations regarding information selling to avoid increasing costs for other consumers and the general public. Stakeholders also expressed various opinions on the CCPA and did not limit themselves to the rule-making topics contemplated by the CCPA.

The representatives of the Department of Justice took notes and did not respond or comment. They ended the official session early, after about a dozen commentators had spoken up, and no one else raised a hand.

Many hearing attendees stayed for informal discussions in small groups. I sensed a common view that many of the most urgent issues are for the California Legislature or U.S. Congress to address. Views on what legislative changes to ask or hope for in Sacramento diverge: Some business representatives and industry associations are eager to push for various substantive modifications to CCPA requirements that are particularly costly or harmful to their business models, customers or business partners. Others believe that the business community should limit its demands to corrections of obvious errors and seemingly unintended consequences (such as covering employees as "consumers"), but otherwise accept the conceptual requirements of the CCPA to avoid far greater risks to businesses: perceived "watering down" of the CCPA could provoke another ballot initiative and parliamentary trade-offs could bring back a right to private action.

Some privacy advocates welcome the comprehensive disclosure requirements in the CCPA. If the CCPA comes into effect largely with its current, broad scope, many other California statutes can and should be repealed to avoid duplications, conflicts and unnecessary complexities.

With respect to submissions to the attorney general's office, some business representatives seemed wary about the risks of alerting the enforcement agency to particularly difficult compliance challenges arising from the CCPA. Legal counsels are particularly concerned about the effects of a provision in the CCPA, which provides that any penalty for violations of the CCPA and proceeds of any settlement of an action shall be deposited in a new "Consumer Privacy Fund" with the intent to fully offset any costs incurred by state courts and the Attorney General in connection with the CCPA.

There will be further forums in San Marcos (Jan 14), Riverside (Jan 24), Los Angeles (Jan 25), Sacramento (Feb 5) and Fresno (Feb 13). The Department of Justice team is also inviting comments via email at PrivacyRegulations@doj.ca.gov (<mailto:PrivacyRegulations@doj.ca.gov>)

Photo credit:

[johrling](https://www.flickr.com/photos/johanohrling/) (<https://www.flickr.com/photos/johanohrling/>)

, [California Republic](https://www.flickr.com/photos/johanohrling/24140153062/) (<https://www.flickr.com/photos/johanohrling/24140153062/>), via Flickr

Editor's Note:

For additional information on the CCPA, please see the IAPP California Privacy Law book and CCPA supplement (<https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/>).

© 2019 International Association of Privacy Professionals.
All rights reserved.

Pease International Tradeport, 75 Rochester Ave, Suite 4
Portsmouth, NH 03801 USA • +1 603.427.9200

The Week in Tech: Countdown to the California Consumer Privacy Act

Companies are figuring out how to deal with a new law that gives individuals the right to see, delete and stop the sale of the personal information about them.

By Natasha Singer

Dec. 13, 2019

Each week, we review the week's news, offering analysis about the most important developments in the tech industry.

Hello, readers. My name is Natasha Singer. I'm a technology reporter covering privacy and other thorny industry issues for The New York Times. I'll be bringing you the week's tech news.

But first, a data rights update: As the holidays approach, some families may be counting down the days to Christmas with Advent calendars. Many tech companies, on the other hand, are counting the days they still have left to figure out how to comply with a sweeping new law, the California Consumer Privacy Act.

The law, which takes effect on Jan. 1, will give Californians the right to see, delete and stop the sale of the personal information that companies have compiled about them.

The new law applies to businesses operating in California that collect personal information for commercial purposes and meet certain conditions — like collecting the data of 50,000 people or more. That means it will cover scores of tech companies, app developers, websites, mobile service providers, streaming TV services — as well as brick-and-mortar retailers, drugstores and many other businesses.

The effort has national implications. Companies like Microsoft have said they will honor the data rights in the California law for customers nationwide.

**The perfect gift for everyone on your list.
Gift subscriptions to The Times. Starting at \$25.**

To prepare for consumers seeking to exercise those new data rights, many companies told me they have had to restructure the way they handle users' information. It's not Y2K. It's YCCPA.

I've spent the last week talking to tech executives and legal experts about a few parts of the law that are so new to the United States that many companies are still working out how to comply with them.

The California law gives individuals a new right to see the specific pieces of information that companies have compiled about them. That includes inferences and categorizations — Status Seeking Singles, Blue Collar Comfort, Tight Money — that some companies use to classify people.

Does this mean Uber and Lyft will now be obliged to provide riders in California who request their personal data with a list of all the passenger ratings drivers give them after each ride? Will Amazon be required to give Prime customers detailed activity logs of their streaming video use? Will smart-mattress companies have to show sleepers moment-by-moment records of their tossing and turning?

“Yes, they have to come back with the specific pieces of personal information,” said Mary Stone Ross, a technology consultant who helped write the ballot initiative that led California to enact the law. “So if they're collecting that, your sleep information, they have to respond with it.”

The California law's definition of “selling” personal information includes sharing it for nonmonetary compensation. And the law requires companies “selling” personal information to give consumers the choice to opt out of having their data sold or shared for commercial gain.

Will much of the digital advertising industry, like apps that share user data in exchange for targeted ads, now be obliged to offer consumers a way to opt out?

“There are lots of information exchanges going on in the economy where people don't pay with cash but there's some kind of consideration for it,” Lothar Determann, a lawyer at Baker McKenzie who specializes in privacy regulation, told me. “And all of that is to some extent covered by this very overbroad law.” (Mr. Determann said he was speaking generally, not about any particular company.)

The law gives employees in the state some new rights related to the data their employers collect about them. How does this change business subscriptions to The Times. Starting at \$25. X

Until now, Mr. Determann said, employees in the United States typically received “a notice saying that ‘you shall not have any privacy expectations at the workplace — we record and monitor everything for compliance and harassment, trade secret protection purposes,’ and so on. **The perfect gift for everyone on your list.**”

But as of Jan. 1, he said, employers in California must give contractors and employees a notice explaining the types of information the company collects about them and for what purpose. That is, he said, “something that employers in the U.S. never had to do.”

I’ll be following these new employer data disclosures. So please email me at nsinger@nytimes.com or DM me @natashanyt if you work in California, have already received your employer’s disclosure and want to share it.

Some tech companies say the new privacy law is too broad and prescriptive. Microsoft said it would like to see an even more comprehensive privacy regime. How so?

“California is a good first step because it has some very important rights built in around user control,” Julie Brill, Microsoft’s chief privacy officer, told me. “But too much of a burden has been placed on individuals. We need to ensure that companies share the burden to protect individual data in the United States.”

“That means things like requiring companies to assess the data that they have and to make sure that they’re adequately protecting it,” she added. “It should include privacy by design. Good stewardship requirements should also include principles like data minimization.”

Silicon Valley is not alone in having to contend with a new data rights law. As my colleague Vindu Goel reported this past week, India is set to enact data protection regulations that would give its population of 1.3 billion people some controls over their information.

The Indian data bill is an outgrowth of a Supreme Court decision that established a constitutional right to privacy in the country in 2017. Yet the effort is contentious.

The proposed law would give Indians more power over the details that companies compile on them. But it would also “place fewer restrictions on the government’s own use of sensitive data on its residents,” Vindu wrote, “which include the fingerprint and iris scans that are part of the Aadhaar national ID system and its detailed surveys of who receives government benefits in every household.”

2020 is shaping up to be a very interesting year as American tech giants face an increasingly balkanized landscape of data protection regimes in different countries and, if other states enact versions of California’s privacy law, at home as well. We’ll be covering industry efforts to push Congress to pass a federal law to standardize company obligations — and override some of the data rights that Californians have just gained.

Some stories you shouldn’t miss

- **A number of high-profile foundations** — including the Ford Foundation, the Hewlett Foundation and the Economic Security Project, led by the Facebook co-founder Chris Hughes — are financing an antitrust movement against Big Tech, my colleague David McCabe reported. Can they build momentum for trustbusting?
- **Speaking of tech giants**, an article in Washington Monthly argued that Amazon, Apple and Google should stay out of health care. The piece, by Matthew Buck of the Open Markets Institute, said the tech companies’ drive to maximize corporate revenues could skew the development of health technology away from the best interests of patients and toward overtreatment.
- **Do you own an Amazon Ring doorbell cam?** A sobering look at the monitoring system in Vice called Ring “America’s Scariest Surveillance Company.” Meanwhile, a piece in Slate urged Ring owners to post a disclosure notice for passers-by and offers some mock-ups. One said: “Smile! You’re on a Ring Camera!”
- **An essay in The Atlantic riffed on the meaning of drunk texts** and their rise as a popular communication style. “Like all texting, drunk texting is a form of nonintimate intimacy,” Kaitlyn Tiffany wrote in the piece. “Like all drunk communication, it’s susceptible to poor translation, missed meanings, embarrassment and horniness.”
- **File under the annals of technology:** George Laurer, the man who developed the bar code, could not believe how ubiquitous it became, a Times obituary of the inventor reported. Officially called the Universal Product Code, it made its debut in 1974 when a scanner registered 67 cents for a 10-pack of Wrigley’s Juicy Fruit chewing gum at a Marsh supermarket in Troy, Ohio.
- **Computer science, the most popular major** on many campuses, takes perseverance. This Twitter thread chronicled how one female undergraduate made it through — the A.P. Computer Science “brohort” notwithstanding.

- **A law professor, Frank Pasquale, says** the time has come for a second wave of algorithmic accountability. “While the first wave of algorithmic accountability focuses on improving existing systems,” like tackling bias in facial recognition, he wrote in a blog post, “a second wave of research has asked whether they should be used at all — and, if so, who gets to govern them.”

How are we doing?

The perfect gift for everyone on your list.

We'd love your feedback on this newsletter. Please email thoughts and suggestions to bits_newsletter@nytimes.com.

GIVE THE TIMES

Like this email?

Forward it to your friends, and let them know they can sign up here.



[Tom Kemp](#) is a Silicon Valley-based author, entrepreneur, investor, and policy advisor. Tom is the author of [Containing Big Tech: How to Protect Our Civil Rights, Economy, and Democracy](#). Tom was the founder and CEO of Centrifly, a leading cybersecurity cloud provider that amassed over two thousand enterprise customers, including over 60 percent of the Fortune 50. For his leadership, Tom was named by Ernst & Young as a Finalist for Entrepreneur of the Year in Northern California. In addition, Tom has served as a technology policy advisor for political campaigns and advocacy groups, including leading the campaign marketing efforts in 2020 to pass California Proposition 24 (the California Privacy Rights Act) and advising and contributing to state privacy bills in 2023 such as California SB 362 (the California Delete Act) and Texas SB 2105.

LOTHAR DETERMANN



Lothar Determann practices and teaches international data privacy, technology, commercial and intellectual property law.

At Baker McKenzie in San Francisco and Palo Alto, he has been counseling companies since 1998 on data privacy law compliance and taking products and business models international. Admitted to practice in California and Germany, he has been recognized as one of the top 10 Copyright Attorneys and Top 25 Intellectual Property Attorneys in California by the San Francisco & Los Angeles Daily Journal and as a leading lawyer by Chambers, Legal 500, IAM and others. For more information see www.bakermckenzie.com. Contact: ldetermann@bakermckenzie.com.

Prof. Dr. Determann has been a member of the Association of German Public Law Professors since 1999 and teaches Data Privacy Law, Computer Law and Internet Law at Freie Universität Berlin (since 1994), University of California, Berkeley School of Law (since 2004), Hastings College of the Law (since 2010), Stanford Law School (2011) and University of San Francisco School of Law (2000-2005). He has authored more than 150 articles and treatise contributions as well as 5 books, including *Determann's Field Guide to Data Privacy Law* (5th Edition, 2022, also available in Arabic, Chinese, French, German, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish and Vietnamese) and *California Privacy Law - Practical Guide and Commentary on U.S. Federal and California Law* (5th Ed. 2023). His *Field Guide to Artificial Intelligence Law* is scheduled to be published in January 2024. Recent papers include [Healthy Data Protection](http://ssrn.com/abstract=3357990) (<http://ssrn.com/abstract=3357990>), [Electronic Form over Substance](http://ssrn.com/abstract=3436327) (<http://ssrn.com/abstract=3436327>) and [No One Owns Data](https://ssrn.com/abstract=3123957) (<https://ssrn.com/abstract=3123957>).